An Abstract Process and Metrics Model for Evaluating Unified Command and Control
A Scenario and Technology Agnostic Approach

Author - Jack Lenahan
Office of the Chief Engineer
Space and NAVAL Warfare Systems Command
Charleston, S.C.
Phone: 843-218-6080
Email: John.Lenahan@Navy.mil

Abstract

Purpose

The purpose of this research is to define a domain neutral, process centric framework and the derivative metrics required to assess process re-engineering effectiveness and capabilities based procurement. The paper focuses on process formalisms, process performance metrics, and in particular emphasizes process effectiveness gains through improved process adaptability.

After completing a thorough reading of the document, the reader should be able to define a process, score the process components, identify gaps in the process, redesign and optimize the process, and make capability based process improvement procurement recommendations based upon the process metrics scores. The abstract metrics in this paper can also be mapped to measurable quantities for Agile C2 and Network Centric Warfare metrics classes.

Results

The author believes that he has satisfied the primary goal of this paper which was to describe the methodology and the metrics necessary to assess any set of processes. The assessment score metrics derived from using the approach in this paper can then be used to properly defend the procurement of a process enhancing capability.

"In Ipsa Mentis Luce Veritatis" [St. Augustine, De Trinitate]

Acknowledgements

I would like to acknowledge the following people who have provided assistance, encouragement, and suggestions for this effort to define capabilities based assessment metrics which can be used to analyze and measure adaptive, transformational processes and resources in a Network Centric Warfare Environment. First, the Chief Engineer of the Charleston, South Carolina Center for Space and NAVAL Warfare, Mr. Phil Charles. Phil has provided a masterful leadership model in the era of U.S. force transformation. Second, the management and staff of the Unified Command Structure Project, including Captain Don Diggs, Glen Stettler, John Keathley, Robert Regal, Don Pacetti, Lt. Commander Phil Turner, Dr. Ray Curts, and Bill Hoffer. It was Capt. Diggs who first requested that I capture several abstract metrics concepts into a white paper which has now become the basis of this effort. Finally, I would like to thank Mr. Terry Mayfield of IDA Corporation and Dr. Raymond Paul of the Office of The Assistant Secretary of Defense for Networks and Information Integration, for their timely insertion of scholarly process centric metrics analysis. But most of all, I would like to thank my spouse Deane.

Disclaimer

The material in this paper does not reflect the opinion of the Department of Defense, the Office of the Assistant Secretary of Defense for Networks and Information Integration, The United States Navy, or the Chief Engineer of the Space and Naval Warfare Center at Charleston, South Carolina. The material presented is only the opinions and research results of the author.

"*It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change*" [Charles Darwin].

***"Therefore, soldiers do not have a constant position, water does not have a constant shape, and the ability to attain victory in response to the changes of the enemy, is indeed miraculous."* [Sun Tzu, The Art of War]**

Background

Sun Tzu's quotation above alliterates the necessity and difficulty in adapting to change in order to achieve victory. It appears to be the nature of American history that "adaptation opportunities" are imposed upon us. Twice in the last 60 years, the United States of America has suffered two disastrous surprise attacks. The first assault was the December 7, 1941 attack on Pearl Harbor and the second assault was the attacks of September 11, 2001 on the Pentagon and the World Trade Center Twin Towers in New York City. The cost [1] of the Pearl Harbor attack was as follows: 2,343 U.S. service personnel were killed, 960 missing and 1,272 wounded; 151 U.S. planes destroyed on the ground and all eight U.S. battleships at anchor in Pearl Harbor were either sunk or damaged. This attack forced the U.S. into World War Two. The total financial cost of WWII is estimated at $2 Trillion over the period covering December 1941 through June 1945. The cost [2] of the September 11, 2001 attack is estimated at 3000 deaths between the Pentagon, the Airline Crash in Shanksville Pennsylvania, and the Trade Center in New York. The September 11, 2001 estimated financial [3] cost at this writing over two years since the attack, is $2 Trillion, including loss of stock market wealth.
The Imperial Japanese Military used a force of 253 aircraft in two attack waves of 183 and 170 planes per wave. The aircraft and the carriers used to launch them were built by the Empire of Japan at a major investment of resources. The terrorists, who attacked the U.S on September 11, required 19 suicide attackers and used 4 hijacked aircraft as Cruise Missiles. The September 11 attackers total cost is estimated at only $1 Million. The hijackers who had no NAVY, no Air Force, no Army, no Space based surveillance, no Marine Corps, and stole all the required resources, inflicted more human casualties in one attack than did the Japanese at Pear Harbor, and the same financial damage in one attack as the entire cost of World War Two. Our enemies would appear to have adapted well.

Pearl Harbor was a traditional or symmetric attack [5]; September eleventh was an asymmetric attack. One of the organizations responsible to assist in force transformation is the Office of The Assistant Secretary of Defense for Networks and Information Integration, and its Command and Control Research Program (CCRP). OASD NII CCRP is encouraging the community to move the study, analysis, and practice of C2 beyond its traditional purpose of uncertainty reduction toward a richer concept of battlespace awareness. To quote Dr. David Alberts "Its charter requires the CCRP to respond to a variety of Information Age challenges. To do so, the CCRP has refocused its efforts to

include new arenas of the military mission space. For example, our focus has shifted from the battlefield to the battlespace, including not only space-based operations and information as a warfare arena, but also C4ISR processes that are integrated across functions, command echelons, and time. The shifts from U.S.-only to coalition operations and from traditional warfighting to a broader agenda, including combating terrorists who may possess weapons of mass destruction (WMD), and Operations Other Than War (OOTW), are also profound. Perhaps the most significant challenge is the transformation of the concept of C2 from a force multiplier (which enables commanders to employ weapons and forces more efficiently and effectively) to a force or central enabler of JV 2020. C2 seeks to enable commanders to defeat adversaries while placing fewer friendly forces at risk and, in ideal cases, actually reduces casualties as well as collateral damage by providing information-based advantages and minimizing adversaries' capacities. The potential for "lockout" and "option dominance" represents a qualitative change in warfare and military mission accomplishment. While systems historically have focused on gathering bits of data and fusing them into information, the systems of the future will generate a rich understanding of the battlespace and facilitate the sharing of this awareness to support decision making, planning, and battle management. Rather than hoping to improve C2 performance, the CCRP is focusing its efforts to improve C2 effectiveness". Another purpose of the OASD/NII is to assist in the implementation of Network [6] Centric Warfare, which is considered as one of the core strategies fundamentally necessary to counter either or both threats. Since one of the promises of NCW is a radically increased joint force utilization capability, the setting for this paper then is to provide a generic framework capable of modeling and measuring the unified command and control processes required to unite and direct the capabilities of U.S. and Coalition assets against both threat types. The primary goal of this paper is to provide sufficient formalisms to derive the process centric metrics necessary to measure whether or not a devised solution reduces organizational complexity, improves process adaptability and therefore improves process effectiveness. It should be noted that a process centric approach is not the only methodology capable of defining metrics needed to measure processes and success in the asymmetric world. However, this paper only covers the process centric measurement approach.

"Act after having made assessments. The one who first knows the measures of far and near wins" [Sun Tzu, the Art of War]

Executive Summary

The purpose of this white paper is to define a domain neutral, process centric framework and the derivative metrics required to assess process re-engineering effectiveness and capabilities based procurement. The paper focuses on processes, process performance metrics, and in particular emphasizes process effectiveness gains through improved process adaptability and improved cognitive capabilities. After completing a thorough reading of the document, the reader should be able to define a process, score the process components, identify gaps in the process, redesign and optimize the process, and make capability based process improvement procurement recommendations based upon the process metrics scores. The abstract metrics in this paper can also be mapped to measurable quantities for Agile C2 and Network Centric Warfare Metrics Classes. The end goal being to determine if military process metrics are improved thus justifying a particular capability's procurement. The figure below depicts the relationships between the classes of metrics as they appear in the appendices following the main paper. However, it is outside the scope of this paper to map from Agile C2 and NCW to military metrics. That is left to those examining a particular process for improvements.

The abstract process metrics should be used to measure whether or not a given process is optimized or "more effective in achieving objectives". This can be accomplished by applying scenarios to a given process model and varying the input volume, input frequency, and input types and then measuring the process in terms of this paper's metrics. Poor process components can then be analyzed and the process itself improved for more optimal process metric's scores.

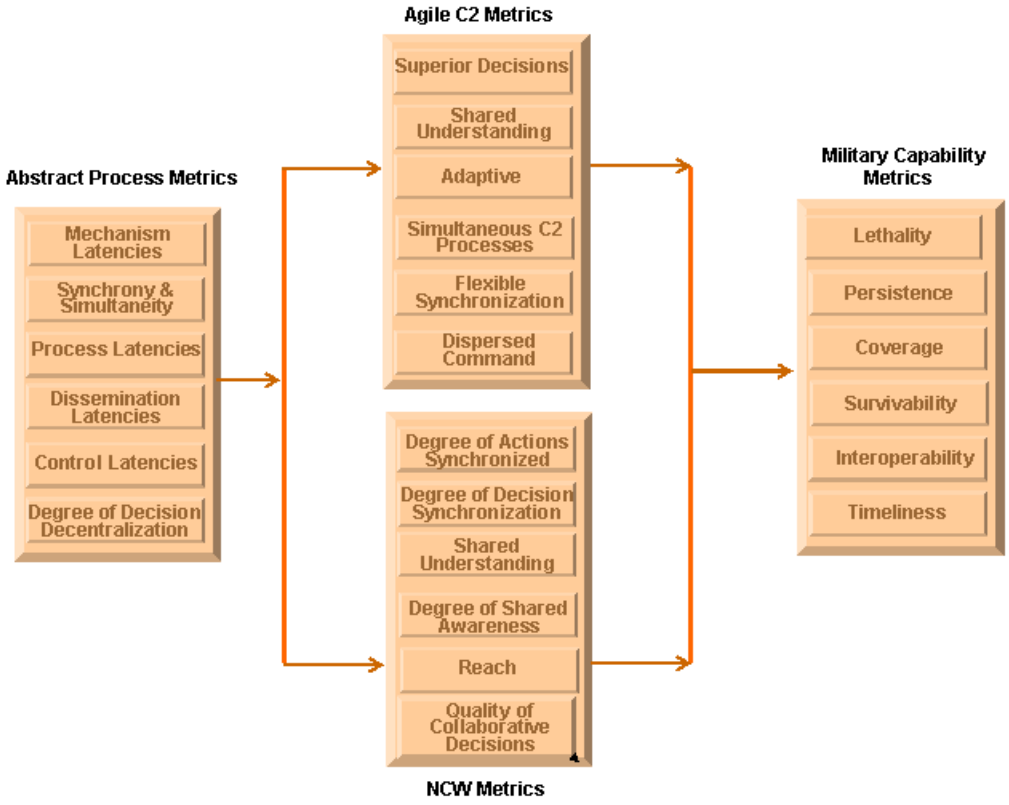


Figure 1 Metrics Classes

If the user is confident that a particular process is optimized, then the user can set about to determine if adding new mechanisms, resources or systems can further improve a process behavior. The new resources or systems must be shown to actually improve process scores against one or more of the metrics in this paper by adding a capability that optimizes process adaptability, reduces many of the process latencies identified in this paper, or improves cognitive capabilities. The user may then show a metrics based justification for requesting that the identified capability be procured. This framework provides the ability for planners to assess the infusion of breakthrough technologies as mechanisms which will improve a particular process's metrics scores.

"Customizing weapon systems to tactics which are still being explored and studied is like preparing food for a great banquet without knowing who is coming, where the slightest error can lead one far astray". **[Sr. Colonels, Qiao Liang and Wang Xiangsui, People's Liberation Army of China: Unrestricted Warfare]**

Introduction

The purpose of this paper is to describe an abstract framework which generically models the ability of decision making processes to generate courses of action, policy or commands in response to or in anticipation of a given set of problems. In order to achieve a scenario and technology free framework, it is necessary to divorce command and control from communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). It is also necessary to divorce C2 from any pre-conceived notions of existing or traditional command and control models. Therefore, the reader should not bias the understanding of this paper with any current theory (Plan, Organize, Direct, Monitor, or Agile C2, or Observe, Orient, Decide, Act, or Plan, Decide, Act, etc.) with which they may have some familiarity.

A primary goal of this paper is to describe the metrics necessary to evaluate any set of processes, policies, resources, and constraints devised to issue a set of commands or control courses of action to address an arbitrary set of input problems. These metrics must be scenario independent (scenario agnostic) in order to properly evaluate the behavior of any proposed command and control (C2) solution model required for policy implementation. Since an ancillary goal of the abstract framework is to assist in process selection, it must also be made clear that the model is to be free of pre-defined domain specific process dogma, such as Six-Sigma, CMM, Business Process Re-Engineering, or any of the myriad of architecture processes available commercially or governmentally. It should be equally understood, that the imposition of "tools in search of a problem" or a "process in search of a problem" prior to a clear understanding of the process requirements and metrics is heretical to the intent of this paper. No solutions or tool sets will be recommended or criticized in this effort. The model in this paper should be used as a C2 process evaluation methodology. Given a scenario from the "real world", how well does the current instantiation of C2 processes behave against the metrics defined in this model?

The framework must also support the modeling of the notion of a primary objective set or a "unifying vision". Given a set of primary objectives, which all policies must target and assist in achieving, the framework must contain a vehicle capable of creating and monitoring the set of policies for consistency with the primary goals. It is important for policy and decision makers to understand in advance if possible, whether or not multiple policies and decisions are synergistic, conflicting, complementary, or degrade the effects of each other. A framework which permits such determinations can be expected to have a "unifying effect" on policy, command, and control. The framework must be capable of optimizing the use of resources from many diverse organizations. A decision maker should be free to use the resources of any military agency, non-military agency, non-governmental organizations, and international organizations.

Instantiating such a framework permits the creation of small teams for minor considerations, or large organizations containing global resources for major undertakings.

A major undertaking will probably require a VIMO, "virtual inter-agency, multi-national organization", capable of drawing upon an extremely diverse and rich set of resources, skills, assets, and experience. For process control and management, I am proposing that each instantiation of the framework as a virtual grouping of resources, contain an embedded Service Level Agreement (SLA), and related Quality of Service (QoS) expectations for the life cycle of the VIMO or virtual organization. The SLA permits formal definition of virtual organizations, terms and conditions for inter-agency resource borrowing and sharing, and closure conditions for the life cycle of the virtual organizations. In process terms, the SLA should contain the "control set" for the VIMO and the "mechanism set" for the VIMO. The QoS agreements should be attached to the SLA clauses as performance metric management instruments. In order to accomplish these goals, the model must enable a methodology for "multi-variable" optimization. One such method for optimization, is the use of vector space mapping topologies, this is the optimization methodology that I have selected for this effort. The variables requiring optimization may be resources, organizations, policies, courses of action, controls, objectives, or any combination of these. The SLA, QoS, VIMO structure, and multi-variable optimizations should be supported by a UCSXML language construct which will enhance the ability to automate many of the functions of the model.

The abstract model will use the following definitions:
a "command" will mean "an order issued to achieve an objective or accomplish a goal", "control" will mean "the management of the issued command".

Why use an abstract model to study C2 only vs. C4ISR?

There are several reasons to extract C2 from C4ISR and to evaluate and study the use of abstraction in the problem solving and policy creation domains:

1. The problem space described by C4ISR is immense.
2. The command and control (C2) space is a meaningful subset of any problem space defined in a military context. It is also much smaller and therefore more manageable than a full problem space describing C4ISR.
3. Abstraction is necessary since studying C2 in a given context (a scenario) will bias the creation of policy, process, strategy, and tools.
4. The abstract model will be useful in the "real world" of C2 to the extent that solution "A" may be meaningfully compared against solution "B" by using the metrics defined in this effort.
5. Process optimization can be enhanced by the use of serial abstract models, parallel abstract models, and hybrids containing various combinations of serial and parallel processes.
6. Many existing legacy systems and capabilities can be evaluated on pure C2 merit alone and not just how well a given process lends itself to NCW style implementations. "C2-ness" can be cleanly compared to "Network Centricity-ness". "Smarter" procurement decisions can therefore be initiated with respect to future C2 capabilities. For example, a given system may be very compatible with the goals of Network Centric Warfare but it may not contain many "pure" C2 capabilities. The reverse is also true. Systems containing a strong C2 suite of capabilities may be difficult to migrate to a Network Centric Warfare environment.
7. An Abstract C2 model can be merged with other abstract models in a more meaningful way than scenario based models. Context free methodologies such as workflow based process models, memetic analysis models, context free protocols, evolutionary learning models, and semantic web knowledge representations can be evaluated in terms of improving or degrading a given process metrics score.
8. An Abstract C2 model permits the modeling of command and control processes which may be necessary due to the failure of data assurance, security compromises, or infrastructure collapse. The abstract model assumes no prior existing infrastructure.
9. The use of the environmental "feedback loop" in the model permits the beginnings of a meaningful definition for terms such as superior decision, lowest level of actionable granularity, shared understanding, and "synchronization". It is also necessary to possess a policy implementation analysis feedback loop to validate the success of policies. Thus, we can create a set of policies which in theory will reduce the number of future input problems. By implementing a proactive policy generation machine, as part of the abstract model, a closed system can be created and simulated. The goal of the policy generation machine is to force an overall reduction in the number, type and velocity of input issues to solve.

10. Virtual Process instantiation as organization can be more succinctly modeled. What is the minimal organization required to ensure successful decision execution or policy implementation? Does the process creation methodology lend itself to the successful instantiation of the necessary organization, policy, and procedures required for successful execution of courses of action, decisions, or commands? UCS can be used to effectively coordinate and optimize all resources of the parent and child virtual organizations while addressing such questions as:
    a. Does a cross-organization resource pool enhance my total available assets or does it make shared understanding more difficult?
    b. Does a common lexicon enhance shared understanding between multi-national and non-governmental organizations or is the time required to develop the lexicon cost prohibitive?
    c. How do I optimize my resource and asset allocations across multiple agencies and multi-national organizations?
11. The use of an organizational construct permits the analysis of notions of "organizational fitness or wellness". Can organization A execute a particular course of action better than organization B.? Can an organization executing Process A produce better, superior, and more understandable decisions than the same organization executing Process B. What would constrain processes to the extent that the process and its organizational instantiation produce fewer successful decisions than another process or organization? This construct permits skill levels, training, and workflow complexity to be evaluated independent of any specific process, organization, or scenario.

"Things should be made as simple as possible, but not simpler". **[Albert Einstein]**

Process and Metrics Foundations

The graphic below represents the foundation process model. Besides reflecting the standard Integration Definition for Function Modeling IDEF [7] structure of inputs, outputs, controls, and mechanisms, this version includes the addition of the process interface as described by H. van Dyke Parunak [8]. A process P_i may be defined formally as

$P_i = <V_i, R_i>$

where

V_i is a set of variables (or nodes) whose assignments change over time, and

$R_i \subset V_i^+ \times t \rightarrow V_i^+$

is a set of rules governing how those changes take place over time.

$\boldsymbol{P} = \bigcup_i \{P_i\}$ is the set of all processes

Basic Sequential Process Model

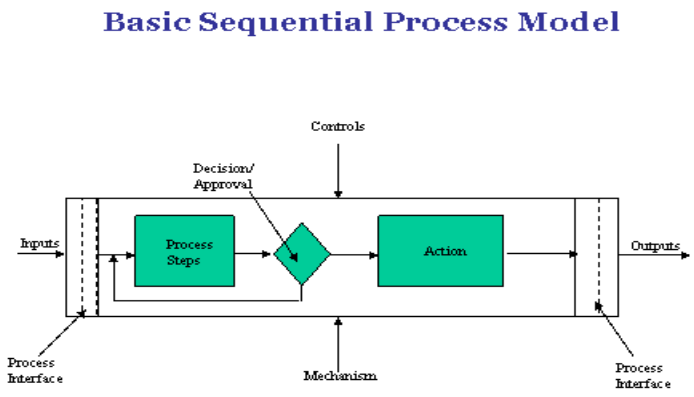


Figure 2 – Basic Sequential Process Model

The model contains the following properties:
inputs, outputs, controls, mechanisms, process steps or tasks, decisions, interfaces, and actions.

Inputs and Input Types

An input is the set of data to be acted upon.

Input types represent the kinds of inputs that are transformable by a given process. In this paper I am proposing the following input types

Managed input type is defined as an input generated as an anticipated result of the process policy or course of action output types. These types should reflect a Poisson distribution pattern.

Un-managed input type is defined as an input not generated as an anticipated result of the process policy or course of action output types. This input type usually has no anticipated set of controls or policy. This input type is capable of severely disrupting the process.

EBO or COA status execution feedback input type is the result of the execution of Policy, or an Effects Based Operations Course of Actions in the environment. This input type usually contains the status of the executing COA or policy, or EBO metrics feedback.
For Effects Based Operations, this type will contain the metric resultant which describes the success of failure with respect to a particular effect or objective, and mechanism usage status of the owning process and the adversary process if known.
There is a degree of uncertainty however in the adequacy of the status information.

EBO Cognitive or Memetic input type is a meme based (see section on cognitive metrics below) which is specifically designed to negatively impact a process either by increasing various process latencies or by forcing a policy change. An example of this was the use of leaflets in Operation Iraqi Freedom to instruct the opposing force of the consequence of using biological or chemical weapons on the invading American forces.

Unanticipated EBO generated negative input type – New input created as a result of unforeseen negative impacts of a given EBO policy or COA. This could be due to poor COA, poor process, or poor execution of COA. An example of this from the Balkan's campaign, is the accidental strike on the Chinese Embassy in Belgrade due to inaccurate data.

Input Characteristics

Input Frequency is the number of problems in a time period, rate of arrival of inputs. For example, the number of inputs or problems arriving at the interface node point per hour.

Input Volume is the number of problems at the input interface at a given time. Could also be defined as the number of inputs in the input queue for processes which use queues.

Input Volatility, variations in the velocity, types, and quantities of inputs

Input Variety is the random arrival at the interface of different input types with random characteristics which will cause the process model to behave differently in terms of end to end performance.

Completeness, Degree to which an input contains all the data necessary to enable input content understanding to the extent that a satisfactory set of courses of action can be recommended to the decision maker. Lack of data will force the analyst to spend time and resources to acquire the necessary data to "complete" their understanding of the problem. At first arrival time of a problem, the completeness may not be known or achievable in an acceptable time period, reflects the percent of data required to develop a good course of action, and also is directly related to the data latency metric and single version of the truth metric.

Known Policy Map Input problem is not new and has been planned for, Number of Policy ID mappings

Complexity is defined as a set of decomposed sub problems. The number of decomposed sub problems required to be created from a given "parent" problem such that each sub problem will receive its own COA or be meaningfully related to a parent COA or policy. The COA's executions will need to be synchronized to permit maximum probability of successful resolution of the parent problem

Intra-input relatedness - Degree of relationships or number of common attributes between inputs or decomposed problems.

Truth content - Is the input data content of input true, false, or unknown? This attribute should include the number of corroborating data sources that a given input interpretation is true.

Actionable Granularity - Is the smallest input data set upon which a process can act

Time Criticality – Input content contains a time constraint for action and resolution, Time measurement = days/hrs. The time embedded in a problem such that exceeding this time, while performing analysis and making a decision, results in an unacceptable outcome or excessive mechanism expenditures.

Urgency Classification of a particular input's relationship to other inputs in terms of which input to address given finite resources to assign for creation of a decision,

implies a spectrum of analyst or decision maker attention – thus some problems will be forced into the analyst's or decision maker's work queues ahead of or behind others – Implies a prioritization and "queuing" of problems to be solved by the analyst or decision maker. This is true of serial or parallel models. Urgency has a classification number from 1 to N, with 1 being the highest assigned priority.

Node Types and Equations

A node [9] in the process is any entity which acts upon the data and is capable of changing the properties of the information flow or the content of the data. Tasks are performed at a node. Tasks may require specialized tasks called coordination, task dispatching, or task and mechanism synchronization. A dependent task is a task which cannot begin until a predecessor task has been completed. Task interdependence is defined as the number of rework links per task. The metric defined for rework links is the dependency ratio, which is simply the number of rework links per task.

A queue is a type of node which is used to store tasks until resources are available or prioritization rules are satisfied.

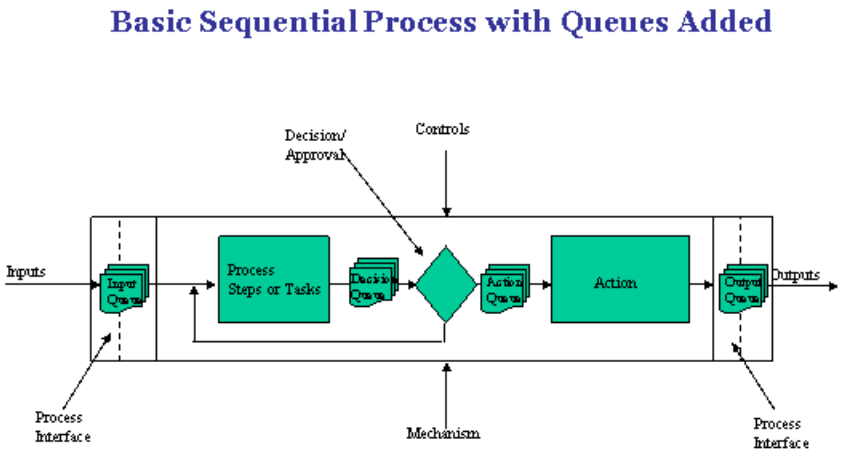


Figure 3 – Basic Process Model with Queues

Queue Arrival Rate – with rate λ

Average input arrival rate $\lambda = \lim t \to \infty$ expected number of arrivals in the interval [0,t]/t

Probability of n queue entries being active at time t = p_n (t)

Average number of active queue entries at time t = (Avg)N (t)

Average delay (avg T_k) of k^{th} entry in a queue being serviced

$T = \lim k \to \infty$ Avg(T)k

Little's [17] Theorem N = λT

Average number N of active queue entries with the average delay T

Queue Waiting Time - $W = \lambda X^2 / 2(1-p)$

Queue Dispatch Rules or Service Strategy – Rule set that defines which queue entry to dispatch to the next node in a workflow sequence. Can be LIFO,FIFO, priority based, or time criticality based.

Node density then is defined by the number of intermediate nodes in the information processing channel [9]. Per process Node Density = Simple Count of Process Nodes 1 to N.

Controls are the rules governing the transformation of data from process input to process output and the sequencing of process tasks.

Span of control defines the number of nodes in a set of processes covered by a particular rule or rule set.

Node rule density is the number of total unique rules required for a particular node to process data (effect a change to its inputs). Node rules usually include a "rule override" capability.

Process rule density is the number of total unique rules required for an entire composite process set to process data (effect a change to its inputs).

Process Data Rules determine how the data is transformed at nodes in the process. They also determine the Policy or COA content and structures.

Process Control rules specify how a node organizes the data to be processed, thus, included in the rule sets are the processing rules. Task dispatching and task workflows are general types of process control rules. Process control rules usually include a "process rule override" capability.
Inputs can be processed in a First In First Out, Last In First Out, or on a prioritized basis. The two main priority types are first, a simple priority assignment made according to a task classification rule set, and second are tasks classified by time constraints. An example of time constraints would be an intelligence intercept with high credibility which claimed that a terrorist attack would occur in 12 hours. Obviously, this type of input should receive a high priority and override other high priority inputs which have no associated time criticality, by definition this becomes a rule described by the formula above and constrains the mechanisms and resources by directing them to a particular task. If a resource was processing a different input task and stopped processing that task to work on the time critical task, this expended time should be accounted for as "**lost task effort time due to prioritization** rules for non-time critical tasks". This can be defined simply as an expended effort lost to task re-prioritization. This is also known as a "**cost of re-prioritization**".
Controls may also represent mandatory contents for an outputs set.

Node Logical Process Control rules determine how a node is to handle multiple sets of inputs, controls, or mechanisms. This can be as a logical AND, a logical OR, or a multi-valued strategy.

Mechanisms

Mechanisms are the resources used to execute an information changing task.

Mechanism Realignment Latency occurs as process latency when a VIMO is assembled but the assigned resources must adapt to new process controls, mechanisms, and centralization structures.

Mechanism Adequacy Metric captures when a resource shortage occurs and a new priority input goes un-serviced, thus staying in an input queue, this time should be accounted for as "task queue time due to resource insufficiency". The metric is simply defined as the task hours lost due to the lack of available resources. It can also be defined as the number of tasks un-serviced due to resource unavailability.

Mechanism Reach Metric captures the ability of a particular resource to be leveraged or accessed by more than one node in a given process, or by nodes in other processes. The metric can be defined as x number of nodes per y processes. For example, if a particular organization had 3000 nodes (computers) which were designated and evenly divided as resources for 30 processes, yielding 100 nodes per process, but only 100 nodes in one of the 30 processes had email, then the reach of the email can be measured in two ways. In the "lucky" process which has email on all 100 nodes, the reach is 100/100, (email reach for that process only). However, organization wide the reach is 1/30 for all possible processes or 100/3000 for all possible nodes. It can also be

used for a singular critical mechanism. For example, a virtual process may be instantiated because there is a shortage of a particular type of mechanism in a parent process. If there are no Farsi translators in the Pentagon, given the proper process controls of a VIMO, the Pentagon Process could reach to the State Department processes via a process interface node and share the resource with Farsi translation skills. Thus mechanism reach applies to mechanism types in general, not just node reach.

Outputs

An output is defined as the set of data transformed from the input data set by tasks, actions, and decisions occurring in the process governed by controls and enabled by mechanisms. Thus an output set can be related to an input set as a pure transform set of input data or as only a relational entity with no one to one correspondence between content of input to output. For example, a large set of data as input which is transformed to a simple yes or no decision as output, such as enormous quantities of sales and production data may be the input to a process which is to decide to build or not build another factory. The decision was based upon the analysis of the volumes of input data, but the volume of data and the format of the output (yes/no) bear no resemblance to the format of the inputs.

Output Types

Courses of Action are plans intended to be executed in order to achieve a specific objective set or maintain an existing policy implementations.

Memetic Effects Based COA – this output type is designed to influence the policies and processes of an adversary in order to impact their decision and analysis latencies such that the adversary changes their policies or processes.

Policy is a line of argument rationalizing the courses of action.

Policy Consistency Checking is the validation that multiple policy segments are not in conflict with each other. The figure below depicts a "Vision" model of multiple objectives consisting of the high level or visionary objectives and lower level policies required to implement the vision level objectives.

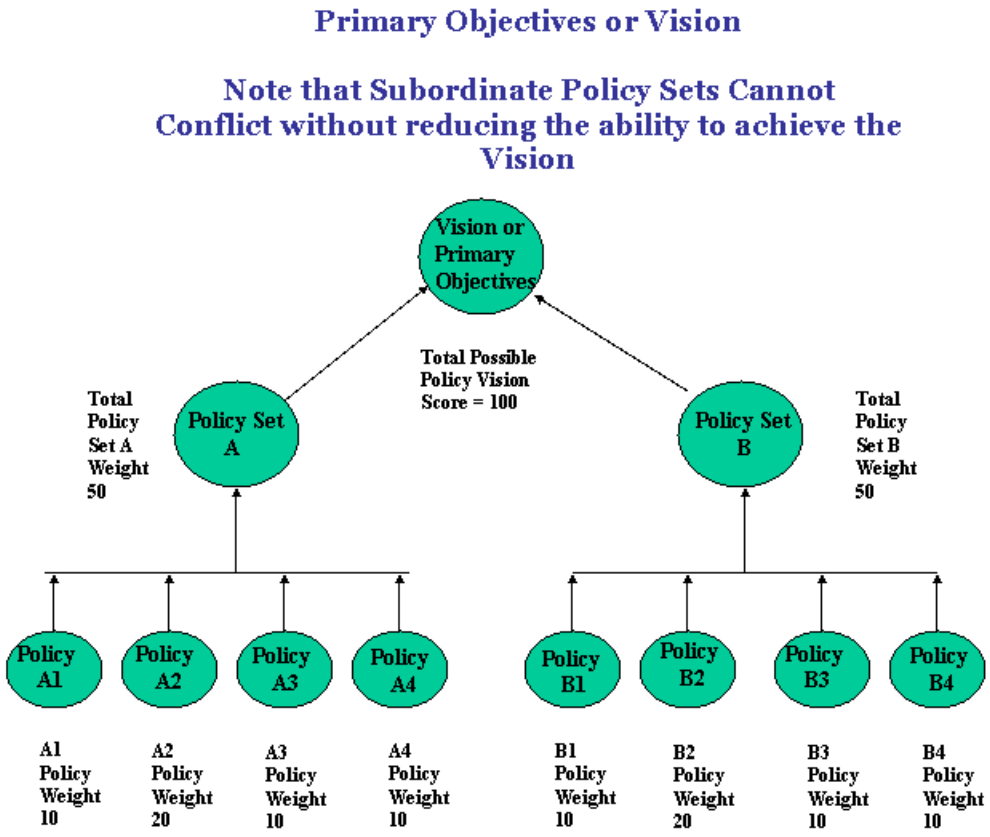


Figure 4 – Policy Interaction Model

It is also important that the analyst understand that any policy or course of action not conflict with or degrade other policies which have been synergistically designed to implement a "vision" or broad set of related goals and objectives. As in the diagram above, if a course of action is the best possible for achieving Policy A3's goals, it may come at the price of being unable to achieve policies A1, A2, & A4. Thus, the total roll up score required for achieving "the vision" cannot be achieved. Therefore, multi-variable optimization is a mandatory recurring theme in the analyst's tasking. The primary task of the COA implementation team is to affect the landing of the decisions into the correct solution space region. By definition this implies that all involved parties clearly understand the problem, the courses of action, the constraints, the decision maker's intent, and the COA implementation methodology.

Process Efficiency Metrics

Process Information flow processing time through the process is described as the time required to complete state transitions at each process node in the set of nodes (variables in the formal formula) constituting a given process for a particular scenario. This calculation must however include per task-node queue waiting times (T), data

latency (dl), analysis latency (al), decision latency (dcl), dissemination latency or workflow latency (dsl), and mechanism availability latency times.
Thus given a sample scenario, and the state of process queues, for each node (N):
Information flow process time = $\sum_{1 \to n} (al_n + dcl_n + dl_n + T_n + dsl_n + mal_n)$

Volume means the total number of inputs to be transformed into outputs or in the case of outputs, the number of outputs generated from transformed inputs.

Variation is the number of different input types presented at the process interface in a given time window.

Relationships This model assumes that there are many possible relationships between an output and the number of inputs, mechanisms, transformations, and control rules used to create it. For example, a one to one mapping of inputs to outputs, or there may be many inputs which are required to create a single output, or a single input can create multiple outputs, false inputs can create one, many, or no outputs depending upon the single version of the truth content, and finally the hybrid mapping version in which many inputs can create multiple related outputs. This metric is critical in understanding exactly how the process generated its output set. Thus, for a given input or scenario ID (S), an output(X) was generated as a function of Input Set(I), Node Density (ND), Control Set(C), and Mechanism Set (M) in Time (T).

Data Latency is the time required to capture all the data required to perform a task at a node[12], see figure below.

Analysis Latency is the time required by the analysts to create the set of courses of action and alternative courses of action.

Convergent Analysis Latency occurs when concurrent process steps focus on the same analysis task but the tasks are either related sub tasks or actual parallel quality control analysis tasks driving towards the same conclusions. In any case, the concurrent analysis latencies must be summed for parallel analysis tasks on the same data set.

Divergent Analysis Latency occurs when concurrent analysis tasks occur using the same data, but the analysts arrive at differing results. This forces rework in terms of reconciling the divergent analysis results.

Decision latency is the time required by the decision makers to approve a node's output data set, send the data set back to the sending node for rework, or authorize the node's change of state. Decision latency can also occur when a node requests additional inputs from other nodes.

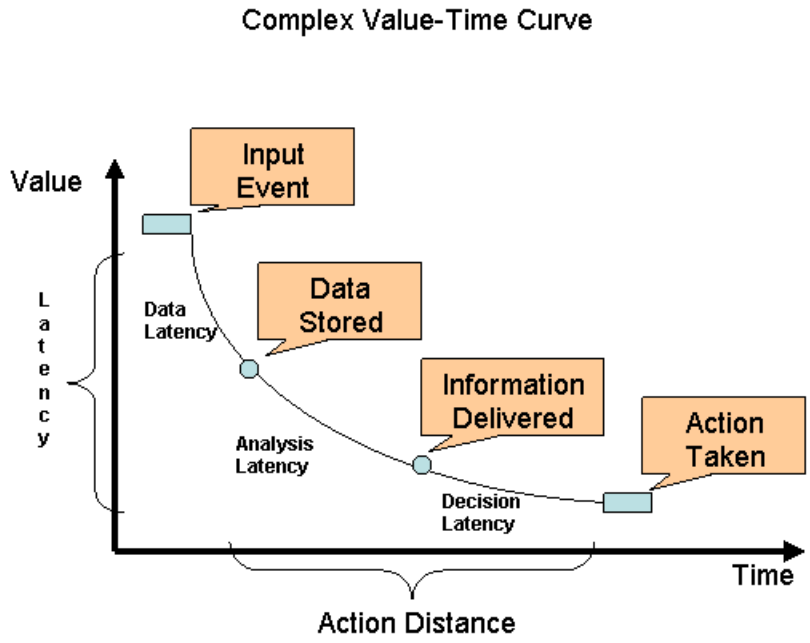


Figure 5 – Action Distance as Sum of Latencies [12]

Action Distance is the sum of all the latencies in a given process set. Thus, AD = the sum of Data latency + Analysis Latency + Decision Latency per process node per process.

Process Service Level Agreements and Quality of Service:

1. Due to the multiplicity of relationships between inputs and outputs, a unique input to output identifier should be created and managed. The following relationships should exist in such an identifier:
    a. Input_Id ~ Output_Id : 1 to many
    b. Output_Id ~ Input_Id : 1 to many
    c. Input_Id ~ Input Types: 1 to many
    d. Output_Id ~ Output_Types : 1 to many
2. Each node should be uniquely identified
3. Each queue should be uniquely identified
4. Controls in effect at each node should be uniquely identified, or governance rules should contain unique identifiers.
5. Mechanisms or Resources assigned at each node should be uniquely identified, or simply each mechanism should contain a unique identifier.
6. For VIMOs, the shared set of 1 through 5 above should be formally defined in a Service Level Agreement. SLAs should exist for any process set which may cross

organizational boundaries. The process interface is thus defined for inputs, outputs, decisions, actions, controls, and mechanisms.

7. For each line in the SLA, a relevant set of Quality of Service Metrics should be defined.
8. The SLA should establish the expected process performance in time based metrics.
9. The SLA should clearly identify the types of inputs to be processed and the expected output types and the expected number of output types for each input type. The SLA should be specific in terms of anticipated input volume, velocity, prioritization rules, and approval workflows.
10. The SLA should contain the controls and resource information transfer context in terms of multiple human languages, mechanism re-alignments estimates (training duration and "learning curve projection to estimate proficiency level expectations for new and re-aligned resources), and learning curve time for resources to adjust to changed control rules or to develop new VIMO specific control rules.

Process capacity is the total volume of inputs that a process is capable of transforming into outputs in a given time snapshot. Process capacity can be exceeded by several primary factors, a simple volume overload at a node, a change in the variety of inputs, unexpected / unmanaged inputs arriving at the interface, or an increase in input velocity.

Node capacity is the total number of inputs that a particular process node can transform into outputs in a given time snapshot within the context of a set of control rules and available qualified mechanisms. Exceeding node capacity will result in an increase of process errors, nodal errors both causing poor output quality which will create rework and increase related queue wait times.

Rework is the processing of the same task more than once at a given node due to errors or poor understanding of the controls or the nodal output user's intent. Rework is by definition an increase in the inputs to a node. A primary source of rework is **Interrupt Driven Task Prioritization**. Rework is by definition a task re-inserted into a queue, rework effort should be considered lost unless it is due to quality process checking. Process design is also affected since task states must be maintained in order to smartly perform the "minimum rework required". The spectrum of rework costs range from a complete restart of the task including a re-acquiring of all resources to fractional mechanism re-tasking.

Node Viscosity [9] reflects the degree of conflict at a node. The conflict arises due to the presence of contradictory information components known as information [9] particles which are the smallest pieces of information which can exist independently and still retain the characteristics of information. In such cases, Viscosity appears in the form of multiple values of information (multiple information flows feed similar information content to a node) that must be resolved before the node can begin processing (Please note that[9] was quoted verbatim from beginning of this paragraph). Node viscosity =

sum of nodal versions of the truth. Refers to the number of versions of the Truth at a single node– Single Version of the Truth calculation = ∑ Number of versions of the truth (multiple inputs referencing same input event but with conflicting veracity content) e.g., at Node "N" input 1 describes event A as true, input 2 describes event A as false, input 3 describes event A as indeterminate in truth content, thus node viscosity or SVT = 3 at Node "N". An SVT number greater than 1 implies increased data and analysis latencies for the process time at a particular node.

Workflow sequence is the rule set defining the dispatching of the flow of information from one node to another node through the process. Workflow sequence rules will route the information from the input interface, to the input queue or some other node type if the input interface is a buffer or a queue, assign a queue task priority, move the information from node 1 to node n according to a pre-defined rule set (e.g., a priority scheme) and handle information transformation errors. Errors can be detected at any node and sent to any appropriate node for correction or rework according to the workflow error routing rules.
In the case of correlation tasks or multiple versions of the truth reconciliation tasks, the workflow may sequence from 1 to many nodes or many to many nodes. The queues may be in a direct path sequence with each task executing node, or task performing nodes may be sequenced according to a process control set which does not use queues but rather drives transformations directly or in parallel from transformation node to transformation node.

Total information flow time in the sequential model is thus the sum of all the serial nodes' processing times. The impact or role of node density becomes very apparent. If there are many nodes in a sequential process, then process efficiency must suffer unless the process designers have already optimized the process for a minimum set of nodes. I will discuss this later in the section on topologies.

The nodal probability of error should be established as the citation that follows. Routine [10] tasks typically have a 0.05 probability of exceptions, and highly innovative tasks have a 0.15 probability (Jinand Levitt, 1996).

Process Decision Making Topology – Hierarchical Centralization vs. Decentralization

A process factor of centralization can be used to study the impact of the decision making structures in a given process. The degree of decision centralization can have information flow bottleneck effects**.** Centralization [10] can be determined by who makes decisions on the project team: low for most decisions made by workers, medium for most decisions made by first level supervisors, and high for most decisions made by the project manager.

Process Viscosity, Turbulent Information flow, and the Organizational Reynolds Number

Project managers can estimate an OR_N for their organization by creating a work

flow diagram to approximate the degree of subtask interdependency and by assuming an error rate that is justified by the level of task uncertainty. Routine tasks typically have a 0.05 probability of exceptions, and highly innovative tasks have a 0.15 probability (Jin and Levitt, 1996). If the estimated OR_N approaches 0.25, a manager should monitor the situation carefully and avoid any changes to the project plan, such as increasing product complexity or shortening the schedule, that would bring the organization closer to the turbulent region. If the OR_N exceeds 0.25, the process parameters should be immediately changed to bring the workflow into the laminar regime. Possible interventions could include decreasing the level of centralization or placing tasks in series to decrease the level of interdependency.

From [10], "we were able to discover a relationship that includes the probability of errors in tasks, the degree of task interdependence, and level of centralization that predicts the "edge of chaos" to occur at an organizational Reynolds number of 0.25. The managerial implication of an organizational Reynolds number is that it can predict the level of organizational risk for a project given its team characteristics and workflow parameters. If the estimated OR_N for a project approaches the turbulent region, management can proactively mitigate the risk by changing project parameters before turbulent behavior occurs.
The following equation was found:
$OR_N = e/C + 0.25 * Log(D) = 0.25$
e: exception rate at inflection, C: centralization factor (low=1.2, medium=1, high=0.8), D: dependency ratio (rework links per task)

"Rework dependency links" cause an exception in one task to create an exception in another dependent task. The level of interdependency of the work process is measured by the "dependency ratio".

An Organizational Reynolds Number of greater than .25 indicates that process redesign is required. The factors which may need adjustment are:

1. Add a mechanism
2. Add a node
3. Decrease mechanism realignment latency
4. Decrease control realignment latency
5. Add a process set
6. Decrease input volume
7. Decrease control rule complexity
8. Decrease process centralization, unless a non-sequential model is scored in which case increased collaboration or command by negation may be indicated as an improvement technique.

Process Interfaces

An interface I_j among a set of processes is itself a process that includes the union of the other processes [8], as well as additional rules R_I specifying the coupling across the original processes:

$$I_j = \left\langle \bigcup_i V_i, R_I \cup \bigcup_i R_i \right\rangle$$

where
the index *i* ranges over the processes in the interfaced set, (the set should include the SLA/QoS as members of the Rule Set *R*)

$R_I \subset \left(\bigcup_i V_i \right)^+ \times t \to \left(\bigcup_i V_i \right)^+$ (the "interface rules") is a set of rules spanning the variables of different processes and governing how those changes take place over time, and

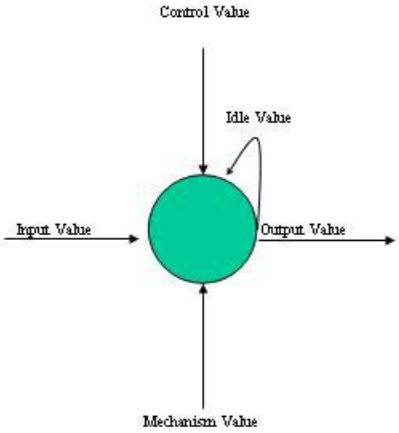
$\boldsymbol{I} = \bigcup_j \{I_j\}$ is the set of all interfaces I_j.

In the graphic above, the interface dotted lines indicate that a process step or state is shared between two or more processes and behaves as an interface process with the rule set being common for all shared processes.

The figures below depict the process node as a finite state machine. Each node is an independent finite state machine which can be viewed as follows:
Inputs: data values capable of changing the state of the node according to the control set rules and availability of resources (mechanisms).
Controls: data values capable of acting as logical control functions for the node.

In the "**Logical AND Node** Model" graphic below, any input value (0,1,2…N) will not be allowed to "flow through the node output unless both the control value and the mechanism values are 1 or true. Thus, mechanisms in this model can also be seen as enablers of the tasks to be performed at this node and controls (processing and data transformation rules) can be viewed as the governance requirements for this node. If either a resource (mechanism) or control requirement is unsatisfied, the output state cannot change. For interface nodes, the rules are shared. Node processing time is thus a factor of the timing of either the presence of mechanisms to perform the tasks or the controls or both. It should be noted however, that there maybe a special controls override condition in which policy or rules permit the creation of outputs at a node in the absence of specific guidance.

Simple “AND” function truth table for process state variable

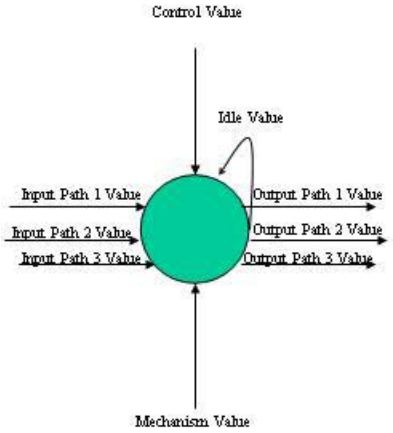


Input	Control	Mechanism	Output
0	0	0	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Note: Idle state = zero in this model but could be designed for any output value

Figure 6 Process Node Depicted as a Logical AND Finite State Machine

Multi-Valued, Multi-Path "AND" function truth table for process state variable



Input Path 1	Input Path 2	Input Path 3	Control	Mechanism	Output Path 1	Output Path 2	Output Path 3
0	0	0	1	1	0	0	0
0	0	1	1	1	0	0	1
0	1	0	1	1	0	1	0
1	0	0	1	1	1	0	0
0	0	7	1	1	0	0	7
7	8	9	1	1	7	8	9
2	4	6	1	1	2	4	6
0	8	9	1	1	0	8	9
9	9	9	1	1	9	9	9
9	9	9	0	1	0	0	0
9	9	9	1	0	0	0	0

Note: Idle state = zero in this model but could be designed for any output value

Figure 6 –A Process Node Depicted as a Logical Multi-Valued AND Finite State Machine

Multi-valued state machine as node type - In the graphic depicted above, each node has multiple inputs, and each input has multiple values. Since the node depicted has only one control rule set for all outputs, unless the control is true (1), and the required resource is also true, all outputs are disabled. Note that this could be designed or implemented in many ways such as a logical "OR". For example, each input could have its own control values and mechanism values. Thus, it would be possible for input 2 to change the state of output 2 given a "true" condition for "2"s control and resource values while at the same time, output states 1 & 3 are disabled. Obviously, the more complex the node rules (controls), the higher the risk of increased node processing time. Reducing the rule complexity or the required mechanisms, can lead to smaller node processing times. It should also be noted again that there may be a case where dynamic node rules permit outputs in the absence of controls.

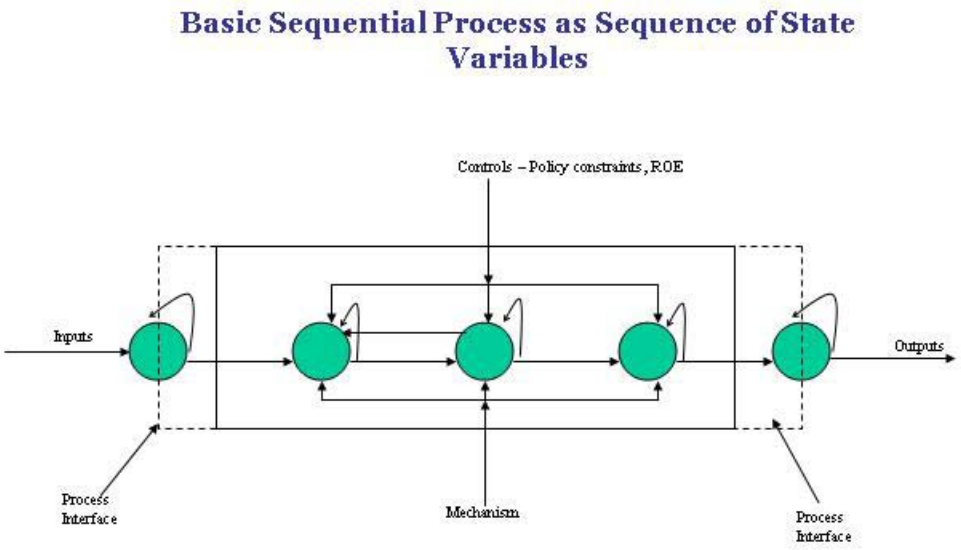


Figure 7 Basic Sequential Process as a set of finite state machines

In the diagram above, the state variable (nodes are variables in the equation set) satisfying the original process set equations, the inputs appear at the interface node (N1), which is also a queue. Next the data is work flowed from Node 1 to Node 2. The second node is the first task processing node. The output of node 2 is sent to node 3, which is a decision/approval node. If the approval of node 2's output is acceptable, the information is then flowed to node 4, if the work output is unacceptable, then node 2 must correct the data content of its output as rework. Node 4 is the action node. The work is then flowed into the output interface queue node, node 5.

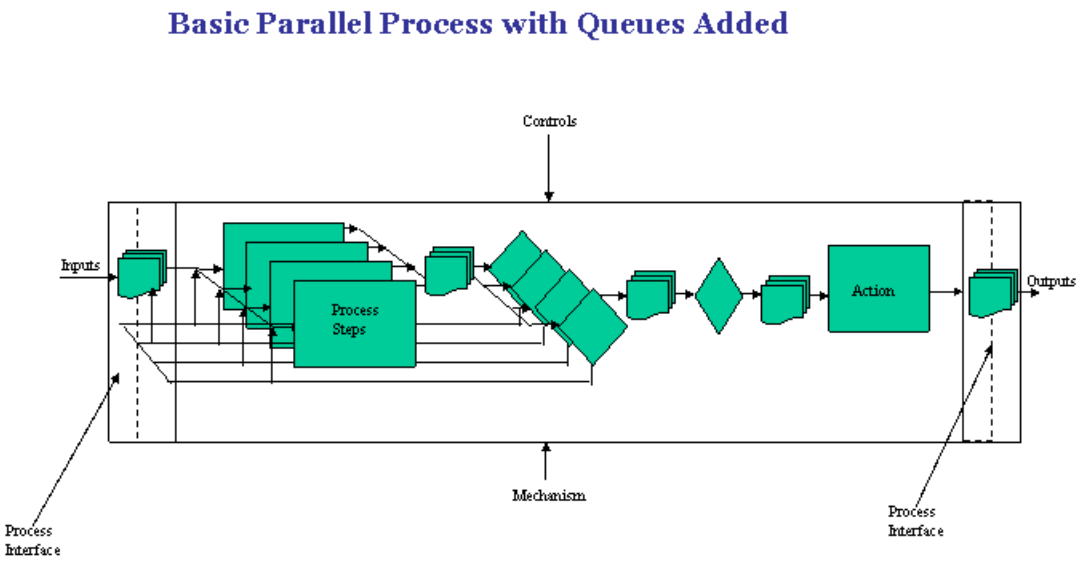


Figure 8 – Serial / Parallel Process Model

A process can also be serial/parallel. The above graphic depicts parallel task nodes, parallel approval / decision nodes and parallel action nodes.

Topological considerations

Interfaces induce a graph-like structure over the set of processes:

$$T = \langle \boldsymbol{P}, \boldsymbol{E} \rangle$$

where

$\boldsymbol{E} = \{E_1, \ldots, E_m\}$

$E_j \subset \Pi \boldsymbol{P}$ is a multi-edge connecting the processes in I_j.

The figure below depicts the correlation of IDEF model to state variable model for purposes of a simple topological description. The state model shows two processes sharing an interface variable value.

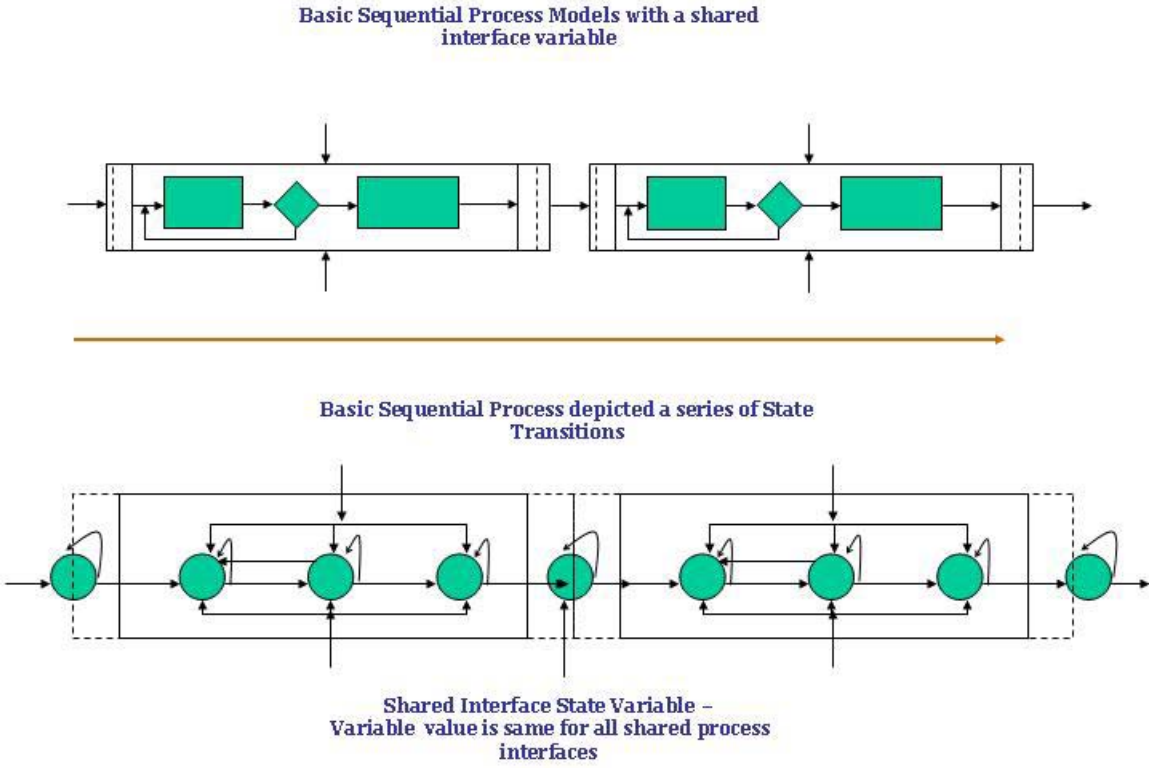


Figure 9 – IDEF to State model comparisons

The interface variable is contains a state value and associated data. For example, the state variable could be "courses of action creation complete = true" and the available data would be the defined courses of action. The state diagram thus depicts the following:

A. Process 1
   i. Node 1 - Interface variable with 3 edges – input, idle, output
   ii. Node 2 – Process Step 1 with 6 edges – input, idle, control, mechanism, output, and rework input
   iii. Node 3 – Process Step 2 with 6 edges - input, idle, control, mechanism, output, and rework output
   iv. Node 4 – Process Step 3 with 5 edges - input, idle, control, mechanism, output
   v. Node 5 - Interface variable with 3 edges – input, idle, output

B. Process 2
   i. Node 1 - Interface variable with 3 edges – input, idle, output

ii. Node 2 – Process Step 1 with 6 edges – input, idle, control, mechanism, output, and rework input
iii. Node 3 – Process Step 2 with 6 edges - input, idle, control, mechanism, output, and rework output
iv. Node 4 – Process Step 3 with 5 edges - input, idle, control, mechanism, output
v. Node 5 - Interface variable with 3 edges – input, idle, output

Using the formula definitions, since we are only concerned with the set of interface edges required to connect the two processes, even though the internal topology has 15 edges, the formula above identifies the inter-process topology as having three edges.

However, we are proposing that it is possible for multiple organizations to compose a single set of processes which will produce a desired output set. In the case depicted below then, the organizations may contain many sets of processes which are required to create an output for a given input. The formulas above describe the graph structure generated if such a process design is used. The set of process connections or graph theoretic edges can be used to graphically depict node density and information flow complexities.

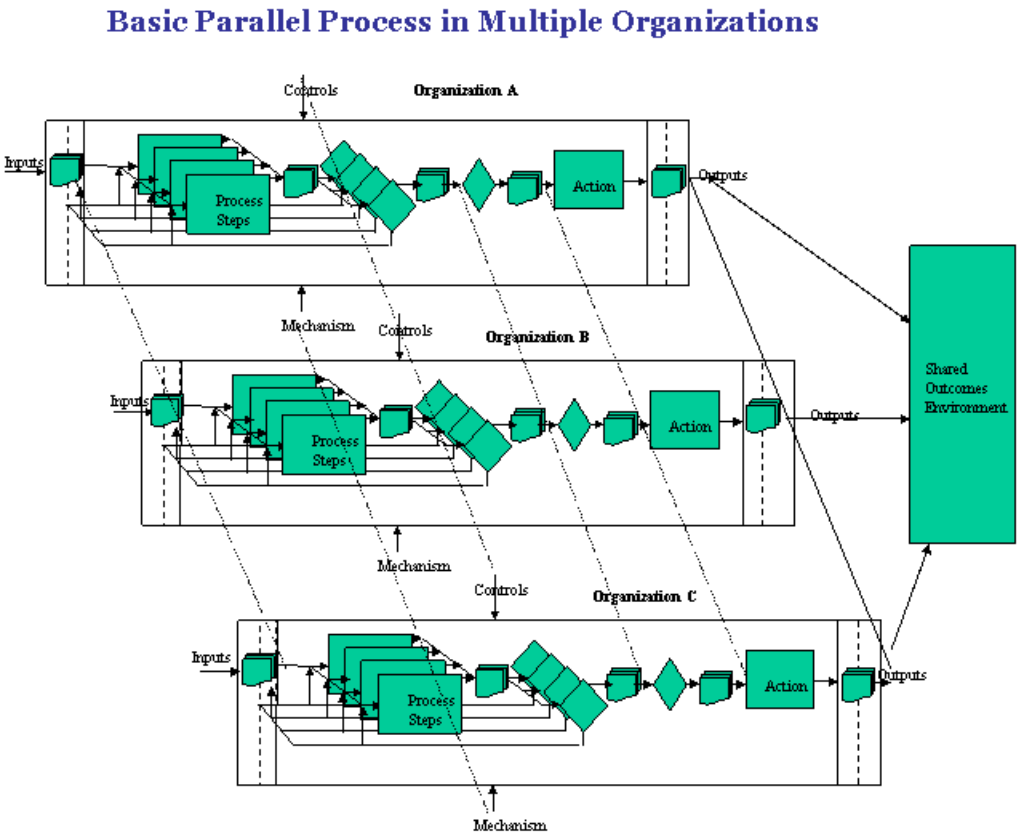


Figure 10 – M Organizations with N Process Steps

The figure above depicts an IDEF version model with M organizations with N process steps per organizational process.

The graph can be used as an analysis tool by process designers to assist in organization and process design simplification.

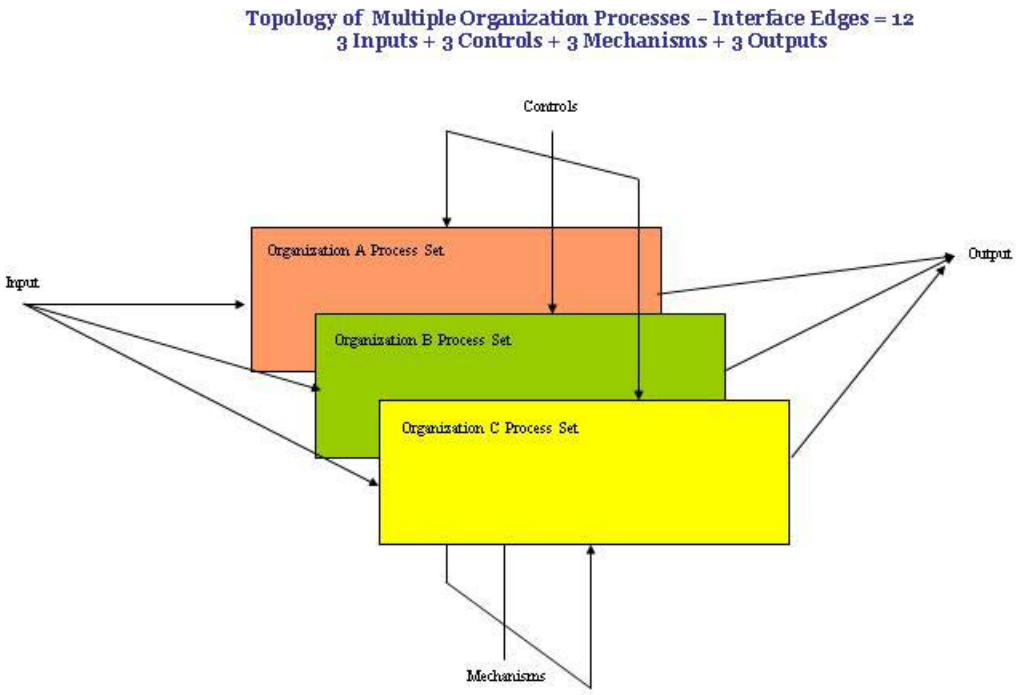


Figure 11 – Multi-Organization Topology

The topology can be used to determine the feasibility of sharing process mechanisms. It can also be used to examine the impact of rule sets on multiple organization information flow dynamics. In the diagram above, a 3 organization process model is depicted. For simplicity, I am assuming a shared mechanism or resource pool and a common rule set. Each process also contains an identical process structure. Thus, there are interfaces between the controls, the mechanisms, inputs, and the outputs, thus 12 edges per the formula above (3 process * 4 edges). An analysis of this type of topology shows several issues. First, most organizations have pre-existing process rule sets defined as controls. This model forces a shared rule set which may conflict with the existing rules in each separate organization. Second, the mechanisms or resources are probably more experienced with their own process controls, other mechanisms (tools) and information flows, thus introducing a mechanism adequacy factor which will add to process latency and throughput delays primarily due to a training related "synchronization delays". Third, an alternative process may be indicated. This alternative will be primarily used to create a Virtual Process divorced of the pre-existing

organization and its controls but free to use the other organizations mechanisms. While this may not immediately reduce mechanism realignment by itself, it will by definition reduce node density and thus the probability of rework due to process errors.

Latencies for a VIMO introduced by using M parallel organizations with N process steps per organization [11] include:

Stimulus Latency – timing that reflects how long the stimulating input takes to reach a particular process interface node as an input. Note that all process interfaces must have been reached.

Input Latency – timing based upon how thick/thin the interface is in order to handle the variation, volume, and velocity of the arriving stimuli prior to entering the specific process

Process Latency – timing across the processes' functional steps to include internal steps only but not interface coordination and synchronization taken to produce the result that appears at the output interface. Process turbulence internal to the process itself, not the interfaces.

Output Latency – timing based upon how thick/thin the interface is in order to handle the variation, volume, and velocity of the output content as they leave the specified process

Dissemination Latency – timing that reflects how long it takes to move the content from the outer edge of the output interface to the input edge of the other process.

Interface adaptation or realignment latency occurs when the controls or mechanism are adjusted so that the manner of receiving and disseminating stimuli changes in order to reduce input and stimulus latency. This metric is measured in time units as a delta from a pre-determined process throughput or node timing metric.

Process adaptation latency occurs when the nodes, process steps, controls, or mechanisms are adjusted in order to reduce data latency, analysis latency, and decision latency. Thus, in order to properly understand adaptation, the reference must be given.

Node adaptability or realignment latency is the time required to change the rule, mechanisms, or states, at a node in order to permit the node to process additional inputs in terms of new data, higher velocity data rates, higher volume, or a different data type. This metric is measured in time units as a delta from a pre-determined process throughput or node timing metric.

Queue adaptability or realignment latency is the time required to change the rule, mechanisms, or states, at a node in order to permit the node to process additional inputs in terms of new data, higher velocity data rates, higher volume, or a different data type or to adjust queue wait times, work dispatch rules, or work prioritization rules. This metric is measured in time units as a delta from a pre-determined process throughput with respect to the queue wait time timing metric. It is intended to measure the reduction in queue waiting time as a result of process re-engineering.

Mechanism adaptation latency or mechanism realignment latency is a time based metric which measures the time required to adjust mechanisms to new roles or processing functions. This metric is measured in time units as a delta from a pre-determined process throughput or node timing metric.

Controls realignment latency or rules adaptation latency is the time per node in a rule span of control that is required for new rules or controls to be understood and incorporated into a process such that the nodes and processes can affect the information flow dynamics or state changes of a node or the approval workflow sequence in a new manner. This metric is measured in time units as a delta from a pre-determined process baseline throughput or node timing metric.

"…in the recesses of the mind, there are various awarenesses of various things, and they come out somehow into the open and are set as it were more clearly in the mind's view when they are thought about[13]". **[St. Augustine, On The Trinity]**

Cognitive Metrics Foundations and Adversarial Shared Process Interfaces

The following metrics are not meant to be an exhaustive set of the so called cognitive metrics. They are to be considered a meaningful subset.

A **Common lexicon** should exist for all resources involved. A lexicon is an agreed upon language and definition set for terms to be used in a given process. The lexicon will enable a "richer" set of shared meanings and assist in the improvement of shared understandings permitting synchronizations to occur. The lexicon at a minimum should contain a set of terms used to define courses of action, tasks, orders, commands, and boundaries (policy constraints or "rules of engagement") for military applications.

Single version of the truth is defined as the melding of truth content for use by the analyst such that no contradictory information exists at any node in a process. The ideal metric value is one with a corroborating value of verified by multiple sources. The higher the numbers of versions of truth content concerning a particular event, the poorer the chance for good cognitive understanding by the analysts and decision makers. SVT as a metric is numeric with a qualifier. For example, the African uranium issue relative to President Bush's state of the union speech. Intelligence Agency A, said as fact that the Iraqis attempted to purchase uranium. Intelligence Agency B, said as fact that the Iraqis did not attempt to purchase uranium. Intelligence Agency C, said that the Iraqis may have attempted to purchase uranium, and Intelligence Agency D, said they could not sort out the truth content that the Iraqis attempted to purchase uranium. In this example there are 4 versions of the truth and not a single version of the truth. Data latency for an analyst and analysis latency for the analyst in this case is high due to the tie attempting to gather the correct data and the analysis required to determine the truth content.

Correctness is the degree to which a system or component is free from faults in its specification, design, and implementation [IEEE 90]. Source: Institute of Electrical and Electronic Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, N.Y.:1990. The metric should be the number of process implementation faults or missing requirements given a process specification.

Consistency, the number or percentage of set data elements that contradict the meanings in the common lexicon. A low contradiction score indicates a high degree of consistency. IEEE - the degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component, [IEEE 90]. Source: Institute of Electrical and Electronic Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, N.Y.:1990

Currency, the number or percentage of data set elements that have common lexicon definitions which have been superceded. *The property of belonging to the current time*: Source is Hyperdictionary.com

Relevance, the percentage of data set elements required to complete a task, that contribute to the final analysis or decision, such that the elements have immediate bearing upon the topic of the task. The relationship of the data sets to the task output such that if this particular data set element were missing, a different conclusion or decision would have been reached. For example, if a data set contains ten elements, but the final decision of a task was based on only 6 elements, then the data set contained 40% irrelevant data. In logic, relevance would mean that a conclusion was of a type non-sequitur if terms in the conclusion did not appear in the major or minor premise. Thus, another relevant metric would be the number of terms in a COA which were not pertinent to the achievement of the objective set.

Accuracy or Precision, percent of content which matches ground truth of a data set. Not a meaningful metric if a data set is not accessible for truth comparison. From Hyperdictionary.com: *the quality of being reproducible in amount or performance.*

Timeliness, availability measured in time, for which data necessary to make a decision arrived or was gathered before the expiration of a time constraint in the input set or the violation of a SLA/QoS condition.

Understandability is defined as the percent of terms in the input, relevant data sets, and courses of action that map cleanly (preferably perfect cognates) to a common lexicon. A score of 100% lexicon mapping is a lofty ideal. This is also related to the issue inter-relatedness, complexity and memetic content metrics in that unique (non related issues), less complex (fewer sub-problems and tasks to be performed), and simpler memetic score issues should require less time to grasp.

Belief systems or Memetic Content Metrics

Several other works addressing so called cognitive metrics use the term “belief system” to describe the dimension of an input problem where it may be significant or meaningful to understand the problem causer’s intentions. In order to attempt to quantify the notion and impact of belief system as a dimension of any problem space, input vector, or policy vector, I would prefer to use the term “meme” [15] instead of the term “belief system”. The notion of a meme, as discussed by Richard Dawkins in his work entitled “The Extended Phenotype”, permits a simple aggregation of complex terms. Memes should be considered a part of the input and policy vectors. Memes are ideas. Examples of memes are democracy memes, nationalism memes, peace memes, Catholic memes, Protestant memes, Fascist memes, Communist memes, or environmental memes. Dawkins believes that memes are replicated like genes and used as generational transmitters of basic cultural ideas. Why, for example, is Ireland 95% Catholic and Israel 95% Jewish? The answer is that the Catholic and Jewish memes are replicated in each respective culture’s educational systems. Thus, the awareness of memes, their number

and intensity, can influence problem understanding, policy creation, and course of action selection. The memes can also be used as a determinant in the establishment of a basis of trust or authority during a policy negotiation process.

The causal impact of memes on the input vector can range from zero to being the source of the problem. Memes can play an important role in the determination of proactive policy. In dealing with a country that is a dictatorship, a policy can be devised to affect a change to that countries memes as part of a broad course of action. For example, courses of action directed at spreading "democracy memes" can be initiated in the hopes of avoiding armed conflict. Thus, actual problems can be addressed as well as potential problems. The problem space model can then contain obvious memetic conflicts which may degrade existing policies and courses of actions. An example of this from World War II was the difficult decision to bomb the Monte Cassino monastery viewed as an historic treasure from a perspective of Catholic memes. The existence of the Catholic memes complicated the decision making process.

An example of memetics as a basis for certain classes of effects based operations.

The memetic metric then is the sum of the unique memes in a given issue or COA. For example, responses to an issue generated by Russia, may involve creating a COA which must address Russian Nationalism, Ukrainian Nationalism, and Marxism. The memetic metric score here is 3. This would usually imply that the COA addresses each memetic member of the input set as a parameter of concern in any proposed solution.
Negative influence memes can arrive at an input queue also. These are adversarial memes designed to influence public opinion or produce economic dislocation in the targeted country. For example, an adversary could leak false information that an attack on an OPEC oil field is imminent. This could cause an adverse reaction in the stock and commodities markets.

The Adaptive Process – An Adaptability Discussion

Few areas in science cause more confusion than the notion of adaptation to the environment. The notion of being responsive to change seems vague and difficult to harness, but perhaps we can make some inroads. The following is provided as a hopeful clarification of the meaning of adaptation in the pure sense, and then how this relates to the use of the term "an adaptive process" or the term "an adaptive mechanism".

In England, prior to the advent of industrialism, a certain lightly colored species, which lived in a lightly colored background environment, successfully managed to avoid its predators and flourish in large numbers. The species flourished in part because the dominant species color was light, and this permitted a natural camouflage with its primary environment, a local set of trees. The darker shaded members of the species stood out against the lightly shaded tree environment and were easily spotted by the predators. The darker shaded members of the species were called "mutations" of their lightly colored parents. Thus, a "mistake" in copying the genetic material of the parents, placed the darker shaded members of the species at a survival disadvantage. The membership in the species of the darker shaded set was always a small percentage of the

total species population. However, the industrial revolution arrived. During the increase in local pollution due to soot from new factories, the trees became coated with dark material. The lightly shaded species members lost their survival advantage since their environmental camouflage was now removed. The dark members now blended well into the new environmental conditions, while the lightly shaded members were highlighted against the new dark background and were quickly eliminated by the local predators. The dark members now lived longer and were able to reproduce in larger numbers and soon became the dominant species member color. The lightly colored members were now the "mutation". The species survived but a particular style of membership dominance changed. How did this happen? The species "adapted" to its new environment only because it had previously produced dark colored members. Had the "mutation" never occurred, the species would probably have become extinct. In other words, chance genetic copying errors, and sufficient diversity in the original genetic material allowed enough species members to survive in the changed conditions. No novel solutions were ingeniously devised by the species in question. Adaptability to the new conditions occurred because the "mechanism set" of the species was rich enough or diverse enough to cope with the new set of environmental inputs.

Human process adaptation must do better. It cannot be left to chance or random mutations. Adaptability must be designed into all segments of a process, including controls and mechanisms. If a new process is to be more adaptable than the old one then we should be able to measure how much more adaptable the new process is. In terms of a process being adaptive, it can be adaptive in terms of adjusting to new inputs, controls, or mechanism types. Adaptability can be measured in terms of mechanism re-alignment latency, controls re-alignment latency, and the ability to produce new outputs which successfully satisfy policy objectives. In other words, the process itself can be adaptive, the controls can be adaptive, and the mechanisms can be adaptive.

Adaptation Metric would be the number of successful process or mechanism adaptations in a given time unit. In particular, how long did it take a process to adopt new controls? How long did it take for a process mechanism set to adjust to new tasking (mechanism re-alignment latency)? How long did it take a process to create outputs given a new input type or input characteristic? (Process adaptability metric)

At this point, I would like to quote extensively from John Holland's breakthrough [19] analysis discussed in his book **"Adaptation in Natural and Artificial Systems".**
"…Because the framework itself places no constraints on what objects can be taken as structures, other than that it be possible to rank them according to some measure of performance, the resulting theory has considerable latitude. Once adaptation has occurred along these lines, it is also relatively easy to describe several, interrelated obstacles to adaptation – obstacles which occur in some combination in all but the most trivial problems:

1. …. The set of potentially interesting structures is extensive, making searches long and storage of relevant data difficult.

2. … Knowledge of properties held in common by structures of above average performance is incomplete, making it difficult to infer from past tests what untested structures are likely to yield above average performance.
3. … Performance is a function of large numbers of variables, making it difficult to use classical optimization methods employing gradients, etc.
4. …The performance measure is nonlinear, exhibiting "false peaks" and making it difficult to avoid concentrations of trials in sub-optimal regions.
5. …Exploitation of what is known (generation of structures observed to give above-average performance) interferes with the acquisition of new information (generation of new structures) and vice versa.
6. … The environment provides much information in addition to performance values (payoffs), some of which is relevant to improved performance."

Evaluating Holland's points from above yields a few interesting process adaptability observations.

1. The set of possible process configurations is massive; therefore a good optimization technique may require initial complexity boundaries.
2. Process structures may be poorly defined and incompletely documented. A well known cause of process failures is the "process hero". He is usually the only individual on the planet who can make a process execute efficiently. The process weakness which caused the failure is of course poor resource depth and process understanding or "shared process awareness". All process participants should understand the process behavior, not just the hero.
3. Classical optimization in terms of hill climbing and simulated annealing may not be the best choice when process evaluations are performed.
4. Genetic algorithms may be a better optimization technique.
5. This is an extremely important optimization observation. It is quite difficult to pry process owners away from simply improving an existing processes' metrics. It must be allowed in the optimization of any process that the current process is so flawed that making its metric's scores lower still does not provide the same radical improvements that an entirely new approach/process may generate. The old process may indeed be ***NON ADAPTIVE***. However, the reverse is also true, it may be the case that no new process can ever be as adaptive as the current version, this is the difficultly in optimizing legacy processes so that they demonstrate higher process adaptability scores.
6. This is also a key point, all environmental reaction data should be assessed, not just the achievement of the process objectives.

Modified Gaia Theory Metrics Hypothesis – The Lenahan Hypothesis

The hypothesis is as follows: that memes behave in a Gaia like manner. Memes attempt to affect and regulate their environment. This is an additional dimension to adaptability peculiar to the human species. In the case of Asymmetric warfare, terrorists attempt to regulate their environment through the sudden and unexpected use of massive violent force, but the memes present in their minds existed for quite some time and could have been monitored for the crossing of a meme-action threshold. By this I mean that certain memetic sets are held at an intensity level so high, that action on the beliefs is

mandatory. The expression of memes in the physical world can be beneficial or destructive. Examples of beneficial meme sets include altruistic memes expressed by organizations such as “Doctors without borders”, The Red Cross, The Red Crescent, or various United Nations Organizations such as the World Health Organization. These memes attempt to exert a positive influence on the environment. Terrorists, however, exhibit destructive meme sets.

There are situations in modern asymmetric warfare which appear to require a departure from traditional “winning strategies”. This means that given the existence of stateless, globalist groups persisting to violently extort civilization for their ends, and also given that since these groups often inhabit large urban areas: containment or minimization of damage may be the best that can be accomplished at present. As disgusting as this may sound, several examples from modern history show that this is indeed the current situation. First, terrorist attacks in Northern Ireland, Israel, Chechnya, and Spain assume dimensions of hit and run attacks, suicide bomber attacks, and the deliberate targeting of civilians. These differ by nature from symmetric warfare models in that fielded armies are not opposing each other with clearly marked uniforms and insignias. These terrorist assaults also persist for years. To select just one model, Israel has struggled for years to attempt to stop the suicide attacks of its opponents, but appears to only have minimized such attacks. The complete elimination of urban suicide terror attacks seems beyond the grasp of current processes and mechanisms or technologies. I am suggesting that a Gaia theory approach may lead to different process designs. These process models may differ from traditional containment strategies in that a new process analysis methodology is suggested by Gaia theory which may be able to interdict the apparent Gaian self organization.

Gaia theory [20] additionally states that organisms both affect and regulate their environment. So called Gaian Guilds that emerge which are self organizing and beneficial to its membership, are of interest to my proposal.

Another definition [20] is “the ability of life to change its surroundings in a manner favorable to life”. If we substitute memes for organisms, and terrorist goals for “manner favorable to life”, **we can state that Gaia memes attempt to affect and regulate their environment**. Thus, from our country list above, we see that the Irish Republican Army, the Palestinians Liberation Organization, the Chechnyan rebels, and the Basque separatists of Spain have independence memes, religious memes, and power memes all active. The authors of the paper cited [20] discuss two Gaia metrics: recycling and control. While their paper deals with natural Gaian phenomena, I believe that we can demonstrate a measurable connection between Gaia and modern asymmetric warfare participants. If the local meme set exhibits a high control number and a high recycle number, then we should be able to identify a meme-action threshold which is predictable. If we can predict the point at which a meme set moves from ideas to indoctrination to action (the action threshold), processes, policies, and procedures designed to interdict the threshold crossing should be hypothetically possible to create and implement.

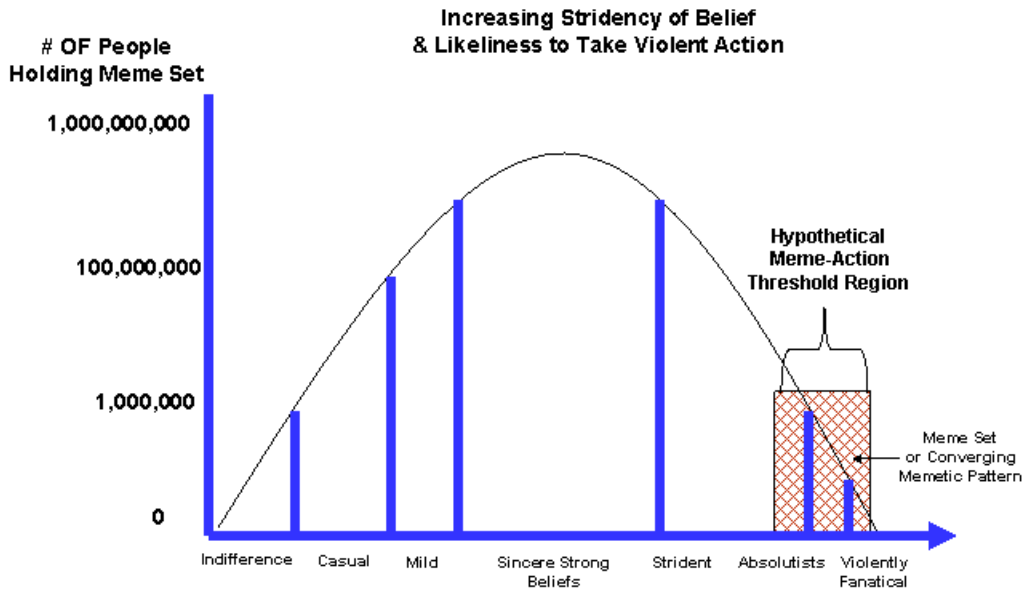
A **Gaian meme recycling metric** could be defined as the number of generations in which a meme set was taught at an institutional level.

A **Gaian meme control metric** could be defined as the number of competing meme sets permitted by the local intelligentsia. If diverse meme sets are permitted, a low control

score, then violence outbreaks should be small. But if no alternative memes or only a few meme sets are tolerated, then the outbreak of violence will be much more likely if the memes exist in an absolutist environment. Dogmatic Ideology memes and Religious memes appear to have a high propensity for crossing the meme action threshold and producing violent behavior.

A **Meme-Action Threshold** then would be defined as the probability of action given a ratio of Gaian recycling versus Gaian control metrics. If a culture recycles it's stridently held ideological or religious memes near a 100% affectivity rate and also controls the appearance of competing memes at near a 100% rate (no other memes allowed), then the probability of attacking a "threatening meme culture" is high.

I believe that too little attention has been paid to memetic influence on process outcomes. For example, how early in the rise of the Third Reich should Hitler's rabid anti-Semitism been taken seriously? These anti-Jewish memes were clearly visible yet ignored. In the case of militarism memes and Pearl Harbor, the Japanese military had already invaded China and Korea prior to their deployment of the task force which eventually bombed Pearl Harbor. Should the defensive processes of the U.S. have adopted a more serious set of protective policies? This author is intuitively convinced (thus the need for the term hypothesis) that there exists a **meme-action threshold** for deeply held convictions at which time action becomes not only imminent but mandatory. One goal of future research using this model should be to run multiple simulations with varying meme intensity levels and action thresholds to determine if violent group asymmetric action or state based military action is highly probable in the short term. The graphic below addresses this. In addition, I am proposing that simple memes regardless of their belief intensity will probably not account for significant and protracted violence levels. On the contrary I am proposing that converged meme sets, containing power lust, ideological absolutism, religious absolutism, nationalism, and materialist memes in some combination could account for the decision to become terroristically violent. There are many belief distribution graphs available in the literature, the model below is mine but hopefully not duplicative of anyone else's research since I am addressing a meme-action threshold. However, if it is duplicative, I will of course resolve the matter and republish with any provided proper citations.



Note that this depicts a "Meme Set", in particular an attempt to bound a meme convergence pattern which leads to violent actions, and does not describe single memes:
For Example:
Absolutist Ideological or Religious Memes, Power Lust Memes, and Materialism Memes can all converge to make a meme set likely to instigate violence. Legitimate test cases would cover the Crusades, the rise of Global Fascism in the 1930's and September 11th for instance.

Figure 12 Meme – Action Threshold

An example of meme based interdiction has occurred in recent history. It is more than interesting to note that in order to stop the spread of NAZI Gaia through the minimization of fascist meme recycling rates and fascist meme control rates, that the Allied Forces in Europe instituted a process of "De-NAZI-fication" in Germany which outlawed the teaching of NAZI theory and propaganda in post war Germany. Thus, fewer new Nazis were likely to appear. Contrast this with the approach of the Roman Army during the third Punic war. The Romans had engaged Carthage twice in the other Punic wars, and were once again facing a long war of attrition. Rome's "solution" was to refuse a surrender offer by Carthage and to kill or enslave the entire regime. Since there was no fourth Punic war, the method, though draconian, was effective. I believe that modern military planners are impacted by the Roman solution and in effect have adopted this style as their "military solution memes". Asymmetric attack participants are aware of this, and rather than directly confront overwhelming military superiority, continue to launch meme attacks in terms of "sympathy meme assaults" through the manipulation of modern media. The asymmetric Guild participant's sympathy memes generate adjusted "process controls" in terms of the strong military state changing its rules of engagement to a posture more favorable to the terrorists. Thus, we have a state "dropping its guard" because it has been influenced by "peace memes" and is now very susceptible to attack by a Gaian Guild with no intention of dropping its meme set or its memetic intensity.

The decision makers intent can be measured in two ways: A simple understanding by all the involved resources such that the COA is correctly executed, or in

a negative way, by a count of the resources lost due to a poor understanding of the COA or commander's intent. The use of this term is amplified by the following [21]: "nesting of Task and Purpose is precisely what military planners try to accomplish to ensure that operations are properly synchronized and focused on meeting the overall commander's intent for accomplishing the mission".

Awareness, shared understanding, and synchronization

The Synchronization metric is really a count of the ratio of the number of potential possible synchronizations to the number of synchronizations which actually occur. The synchronization metric is best measurable as a relativistic metric.
Node synchronization is the number of nodes under the span of control of the same rule set. Thus, the nodes are said to be synchronized by rule set r containing n rules.
Control synchronization is the set of process interface nodes which contain the same rule set.
Mechanism or resource synchronization is the number of set members of mechanisms which are governed by the same rule set for a specific task. This number can be intra or inter process based. It can refer to the same rules of engagement or objectives active at a given time for M mechanisms. **Synchrony** [16] is another name for this metric. In Effects Based Operations, synchrony can result in improved effects scores if executed simultaneously with other specific process tasks to achieve multiple objectives.
Simultaneity then is distinguished from synchrony in that synchrony is the application of mechanisms to the same task in multiple processes or organizations while simultaneity is the application of mechanisms to different tasks but occurring at the same time. Thus, "S" synchronized tasks may be occurring simultaneously. The metric is defined as the number of simultaneous different tasks.

Queue Synchronization is the number of queues in multiple processes which share the same set of active tasks rated at the same priority.

Pay attention to your enemies, for they are the first to discover your mistakes. *Antisthenes*

Shared Adversarial Process Interface – This author is convinced that the modeling of one side of the adversaries in a conflict is inadequate for proper planning. Many shortcomings in asymmetric warfare stem from little to poor understanding of the enemy's Course of Action and planning processes. Option dominance and lockout techniques require thorough planning and adversarial understanding.

Lockout requires that a process COA output contain the necessary steps to prevent the other side from activating response processes or activating response mechanisms.

Option Dominance means that the planning and depth of understanding of the adversary's responses is so rich, that the red plan has in advance "countered" all or most of an adversary's possible response options.

The diagram below depicts the necessary context required to define the terms team awareness, synchronization, and shared understanding. It also depicts a shared interface or adversary interface process or node. This process at a minimum is where adversarial process outcomes in terms of a reduction of mechanisms or an influence of policy occur. Process effectivity this applies to all "3" process sets below: the blue process, the red process, and the shared interface process.

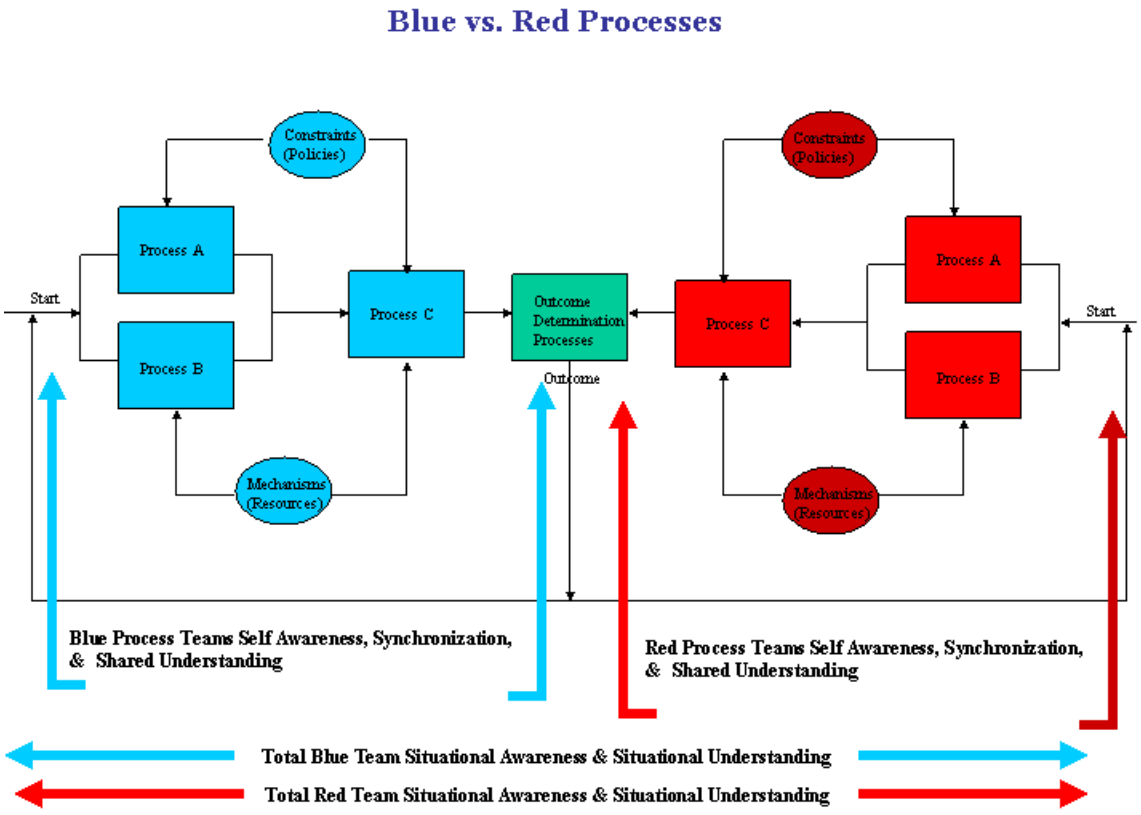


Figure 13 – Comparison of levels of awareness, understanding, and synchronization

If the blue analysts are using processes A&B to co-develop the same set of courses of action and share the same controls and inputs, they are synchronized if they are collaborating together for a single COA recommendation, they share understanding if they are collaborating on the same problem, and by collaborating they are aware of each other, the problem and the proposed COA. The decision maker may not be aware of any of this, in which case the analysts, while synchronized with each other are not at this time synchronized with the decision maker. When the decision maker is presented with the COA for the problem addressed by the analysts, then he is aware of the problem, but unless he is collaborating with the analysts to develop a good understanding, the analysts and the decision makers will not have a shared understanding or be "truly in sync". Now lets take the case where the analyst and the decision makers collaborate through the entire process, then the entire blue team can be said to be "aware", "synchronized", and possess a shared understanding of the "blue process suite and all its steps and outputs. However, unless the blue team is totally aware of the red team's processes, outputs, and intentions, then the blue team does not have total situational awareness, only blue team situational awareness from the receipt of the problem to its decision and COA publication. The figure below depicts a worse case situation to describe total situational awareness at the abstract level.

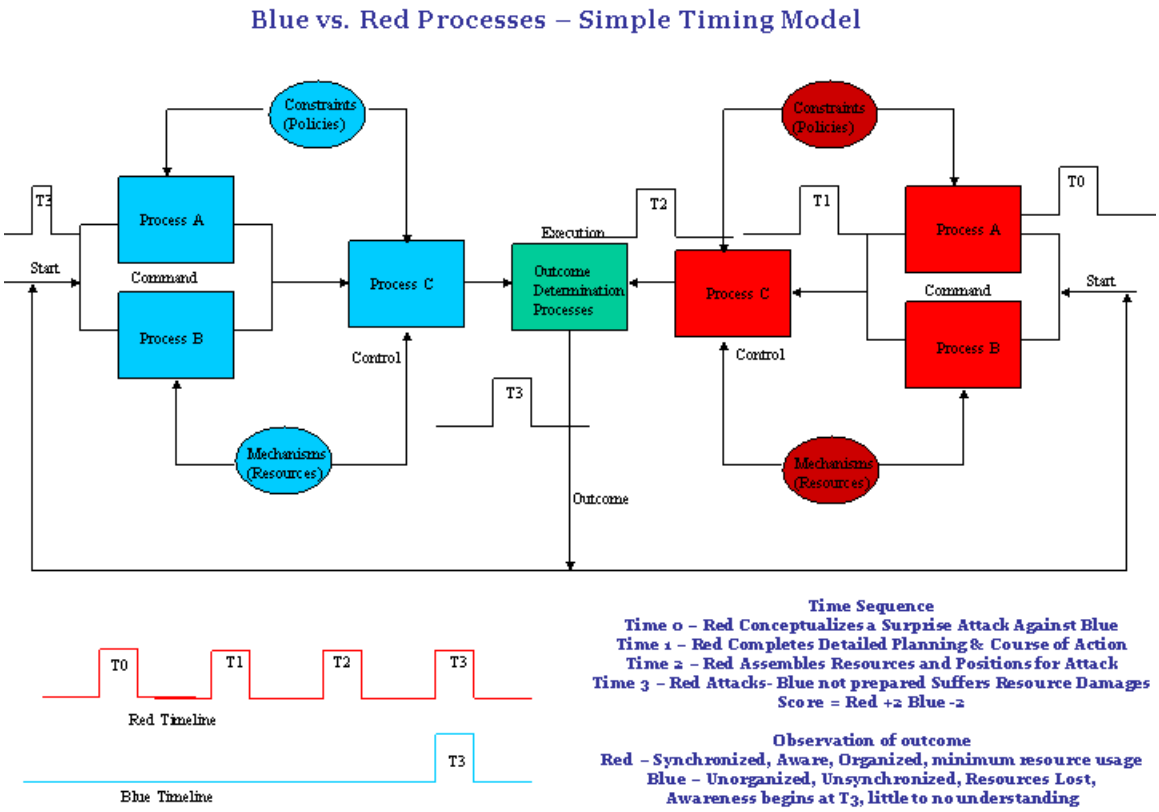


Figure 14 – Timing Sequence for Awareness Modeling

Shared Interface Awareness modeling: As the above graphic depicts, at time t-0, the red team conceptualizes a surprise attack against the blue team. At time t-1, red completes a detailed plan, COA, and assembles the required resources necessary for an attack. At time T2, red positions the resources and at time T3, red activates the attack, catching blue team totally "unaware". Red in this case has total situational awareness, synchronization, and understanding for all time periods zero through three. Blue only becomes aware of the problem at time T3. Any proactive policy required for blue to have prevented this attack, would need to have several factors present:

1. Awareness of the plot no later than T2
2. Resources available to counter the attack no later than T2.
3. The preference would be for blue to have total situational awareness starting at T0.
4. Awareness at T1 is still better than awareness at T2

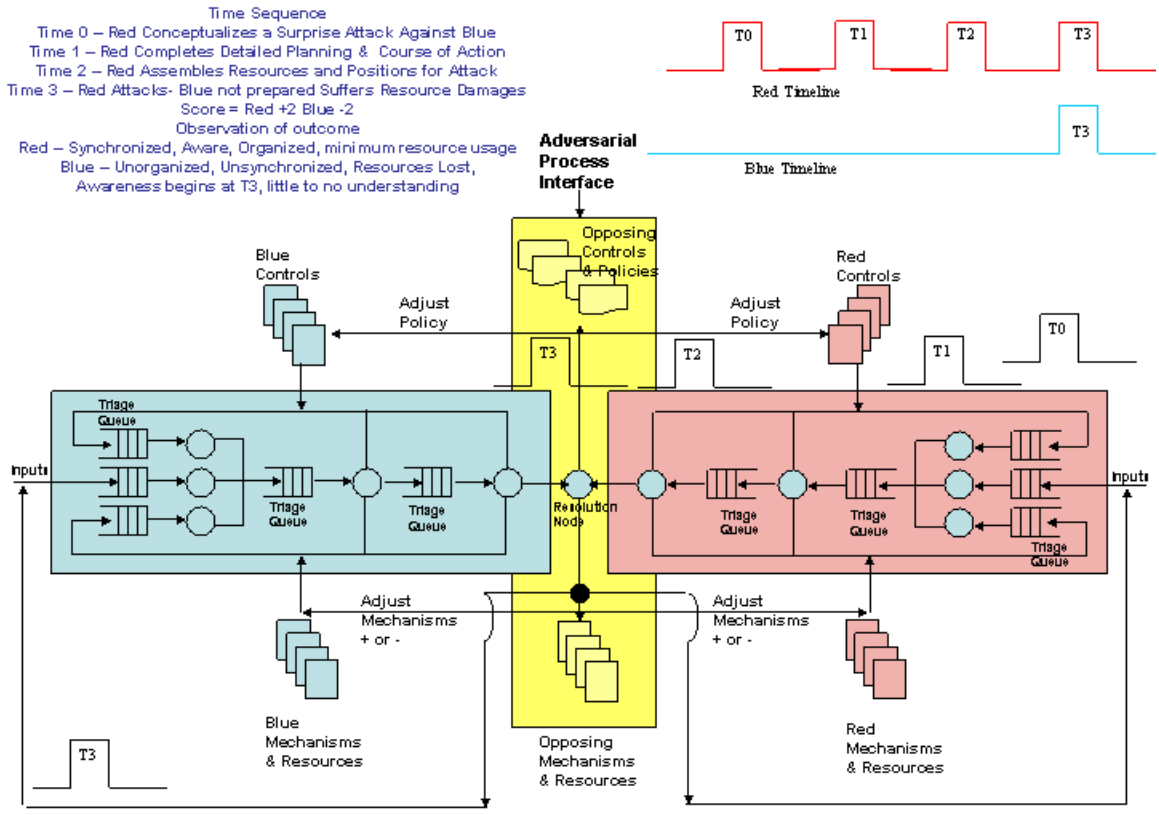


Figure 15 - Another view of the shared adversarial interface using a modified Lenahan – Paul model [21].

5. For Red, in order to insure decision superiority, red should have process steps designed to lock out any significant blue mechanism responses. Failure to design and properly activate the "lock out" activities will possibly result in

Red losing mechanisms unnecessarily. This could also demonstrate the concept of "option dominance".

6. At T-4, not shown above, if blue now reacts quickly after some preliminary analysis, it may be possible to institute mechanism blocking controls which will prevent continued red attacks.
7. To relate this to span of control, the following observations:
    a. Span of control is dominated by Red for Adversarial Process Interface
    b. Red Span of Control is extended to Option Dominance of Blue's Mechanisms management policy
    c. Lockout is used as part of span of control execution policy
8. To use a military example, Don Pacetti [24], a military historian, cites the following criteria:
    a. Red has awareness of Friendly COA and Controls
    b. Red has awareness of Enemy COA and Controls
    c. Red has knowledge of terrain
    d. Red has knowledge of blue force location (mechanism status)
    e. Red has knowledge of red force location (mechanism status)
    f. Blue has knowledge of blue COA & Controls
    g. Blue has no knowledge of red COA & Controls
    h. Blue has no knowledge of red force location
    i. Blue has knowledge of blue force Location
    j. Blue has knowledge of terrain
    k. Red has total situational awareness – blue has no red situational awareness

Relativity of Superior Decision Making

I would like to pose a question at this point. Was the decision to attack by red a "superior decision"? I would like to suggest that superior decisions can only refer to decisions taken in a complete end to end mode (closed system) of a particular activity. In the case of the surprise red attack, red still cannot evaluate the "superiority" of its decisions unless it can manage any blue response without absorbing a high loss of red resources. To put this in a more recent context were Military and Intelligence agency decisions prior to September 11, 2001 "superior"? If "superior", in what context? In order to avoid an endless debate on the relativity of the meaning of a decision's superiority given "n" contexts in unbounded time, I am proposing that we determine either that superior decision making is meaningful only in a given context and a given timeframe or else it should be dropped as a useless metric. If we do not bound this notion of "superiority", then any "superior" decision can be second guessed ad infinitum. For example, the attack on Pearl Harbor could have been viewed as a superior decision at the time of its execution and for some time afterwards.

It achieved an element of surprise, confused the targeted forces, and provided an early advantage to the Navy of the Empire of Japan. Or it could be viewed as a poor decision given the later severe loss of mechanisms/resources by the Empire of Japan. Another example, is the inability of the policy makers the U.S. Congress and Administrations over

the last twenty years to develop alternative energy sources a "non-superior" decision which contributed to the attacks of September 11, 2001? Where are the bounds of superior decisions to be drawn?

Superior or Effective Decision conclusion: If a decision achieves its objectives in a timely manner and according to the accepted COA within the desired mechanism expenditures without violating the controls then it should be considered a superior decision because it was "effective". This should avoid the "relativity" problem.

Stimulation of the Model

Stimulation of processes should consider two basic approaches. The first approach should be to run the model at a Poisson rate. This will permit the base process steps and model to be validated for simple cases. The arrival rates will be steady and the process design itself can be tested for the basic latencies. If a process does not perform well against Poisson stimulation rates it is difficult to imagine that it will perform any better given random, type, volume and velocity rates. This can be thought of as a just in time, rate limiting stimulation rate which tends to focus on basic process efficiencies.

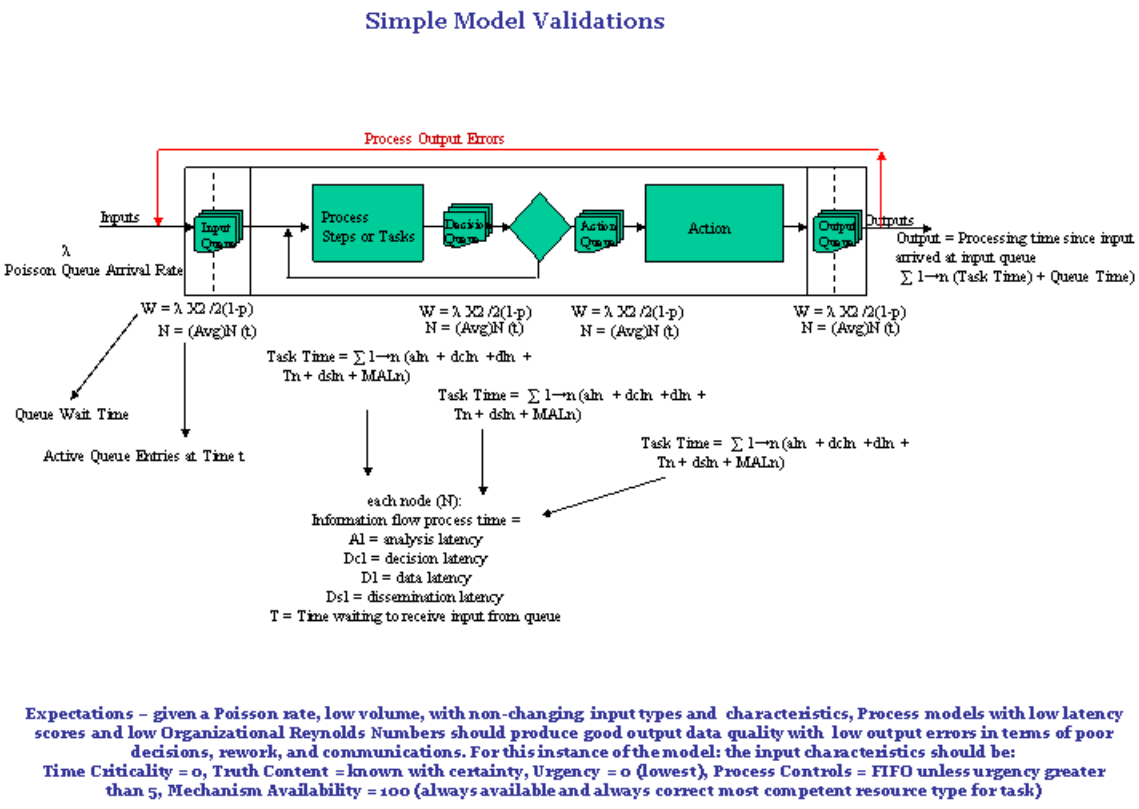


Figure 16 – Simple Model Stimulation

The second approach should be to simulate how a process behaves given a chaotic set of arrivals volumes, and velocities. Chaotic process stressing should include a random variation of the input characteristics. For example, truth content can be randomly true, false, or unknown. The chaotic stimulations can be thought of as "on demand" stimulations. In order for on demand stimulations to produce consistent and stable output flows, the base processes should have been optimized and screened for high Organizational Reynolds's Numbers, high latency scores, and poor decentralization.

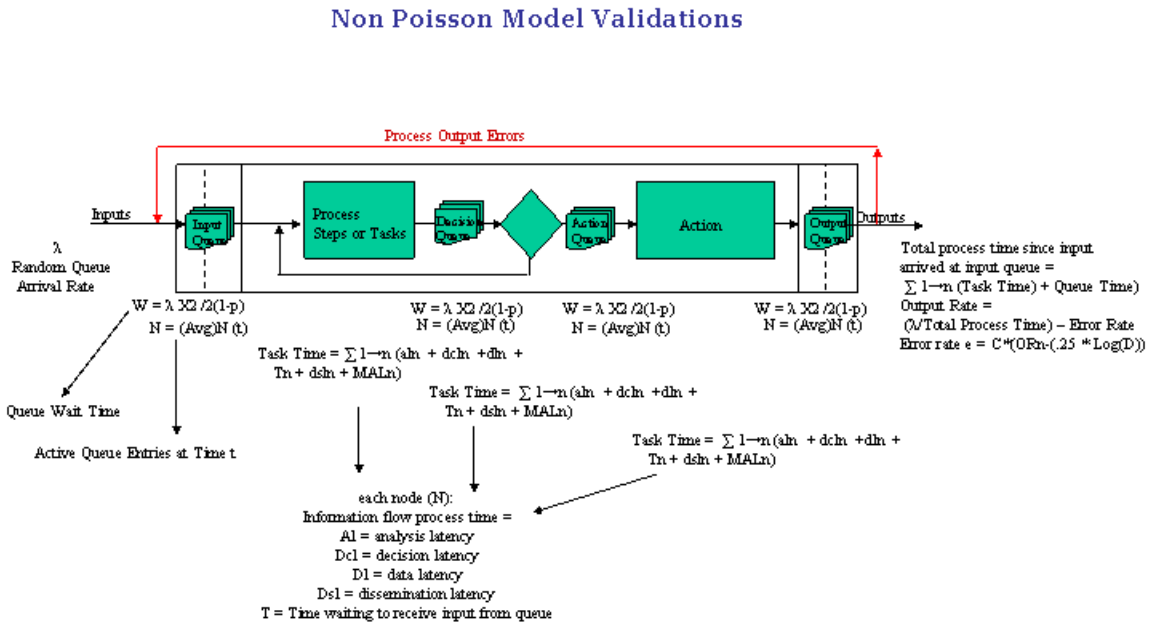


Figure 17 – Chaotic Model Stimulation

Time criticality can be randomized to permit simulation of any time critical scenario. To stimulate the process control rule sets, urgency can be randomized. By randomizing urgency, the input data set becomes unpredictable and should stress the control rules of the process. To stimulate adversarial intent and adversarial influence attacks, meme content can be randomized. This may help to guide policy as to when and where to deploy ISR assets.

Stimulating the model involves several steps.

1. Establish an initial basic abstract process model to be tested. The model must begin with an interface node, at least 1 task queue node, at least 1 process step or task node, at least 1 decision node, and at least 1 action node. Identify the control rule set. This will determine how work is prioritized, enters the queue, leaves the

queue, re-enters the queue, and is processed at a particular node, i.e., FIFO, LIFO, etc. Identify the input data set to be transformed. Identify the complexion of the transformed data set at each node, including the nodal output data set. Identify the mechanism types required to execute tasks at the nodes, identify the mechanism availability rules. Identify the mechanism availability rules per node.

2. Establish the initial process calculations.
    a. Node density
    b. Logical construct of node – (AND, OR, etc.)
    c. Number of rules per node
    d. Max tasks per node in a time interval
    e. Node processing rule model – FIFO,LIFO, Time Criticality task rule
    f. Number of control rules for the entire process – this defines the initial control complexity & span of control
    g. Number of Mechanisms per node – Resource proficiency and re-alignment values
    h. Max tasks per mechanism at a node
    i. Max time duration for a mechanism at a node
    j. Queue Structure – FIFO, LIFO, priority based, time criticality based
    k. Mechanism availability rules per node
    l. Error probability per node
    m. Node viscosity = sum of nodal versions of the truth. Refers to the number of versions of the Truth at a single node– Single Version of the Truth calculation = $\sum$ Number of versions of the truth (multiple inputs referencing same input event but with conflicting veracity content, e.g., input 1 describes event A as true, input 2 describes event A as false, input c describes event A as indeterminate in truth content. Thus, a SVT number greater than 1 implies increased data and analysis latencies for the process time at a particular node. Assume that a single version of truth (1 source only) has an SVT multiplier factor on nodal processing time of 1, that an SVT of 2 doubles, 3 triples, etc.
    n. Process Viscosity or the Organizational Reynolds number
    o. Rework rules for errors
    p. Number of rework edges – Rework Links
    q. Number of serial nodes
    r. Number of Approval nodes
    s. Number of Approval node to Approval node edges – (Hierarchical model indicator if high, Horizontal model if lower)
    t. Number of nodal edges – Indicates inter-nodal & process complexity
    u. Average number of nodal edges
    v. Number of process interface edges - Indicates multiple process complexity
3. Define the input types, type volumes, type velocities, and attributes.
    a. Identify the number of different input types for the particular instantiation of the model.
    b. Identify the arrival rates per and volumes for each input.
4. Determine the queue algorithms for wait time

5. Determine the equation set for queue input arrival and servicing.

A sample process to model and test

In order to assist in the clarification and usefulness of the metrics and process models described above, I am submitting the following model from Terry Mayfield's Dominant Maneuver Work [14]. This section is divided into two groupings. The first section is the IDEF versions of the processes; the second section is the state diagram nodal version. The metrics will be described as required in each section. Also for descriptive purposes, I am assuming that each major sub process will be performed by a separate organization. This will assist in modeling the Virtual Inter-Agency Multi-National Organization Concept (VIMO) M organizations with N process steps each per organizational process.

Modified Version of Mayfield's High Level Dominant Maneuver Process Model

The models below have been provided by Terry Mayfield. I have modified and simplified the models for use as examples of how to utilize the material in this paper.

The process model below has the following characteristics:

A primary IDEF process required to Generate Courses of Action for a new theater consisting of three major sub processes, a process to allocate mechanisms to the other two processes, a process to create COAs, and a process to provide a commander's estimate of the COAs.

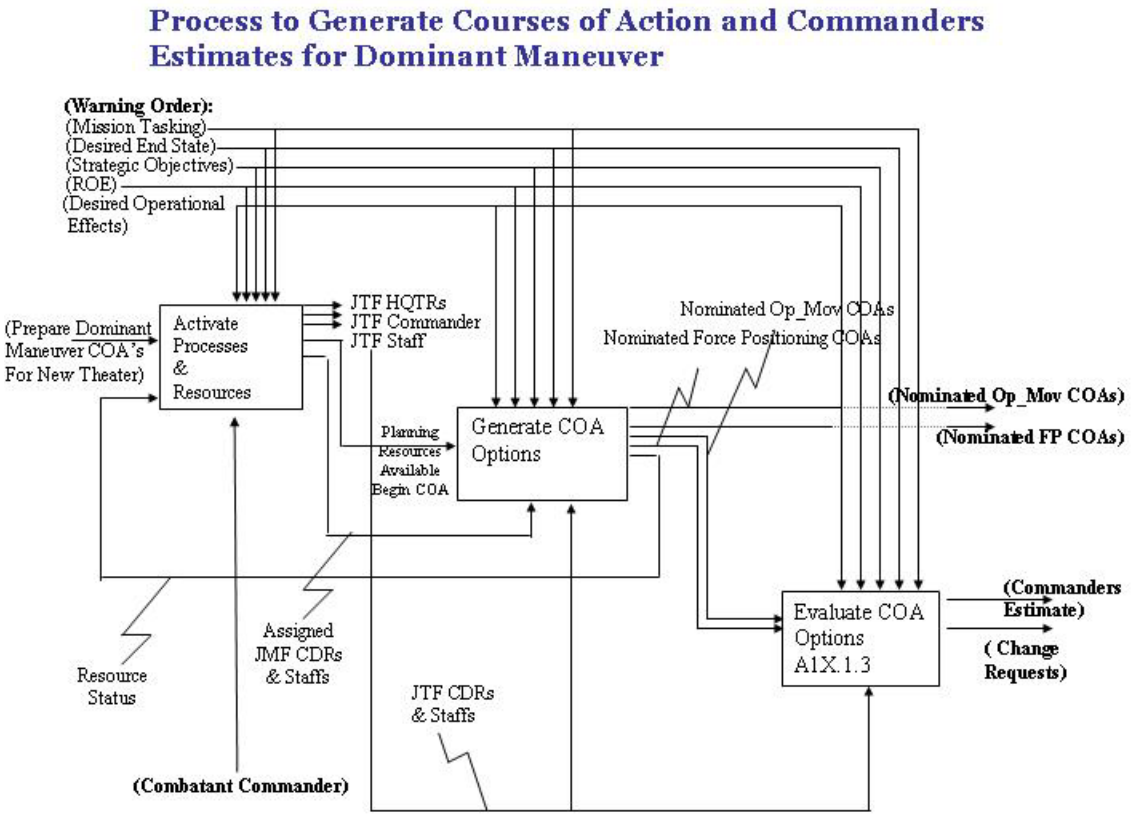


Figure 18 – Mayfield's Dominant Maneuver Model Modified for Concept Demonstration

The first sub process is the "Activate Process and Resource activity".

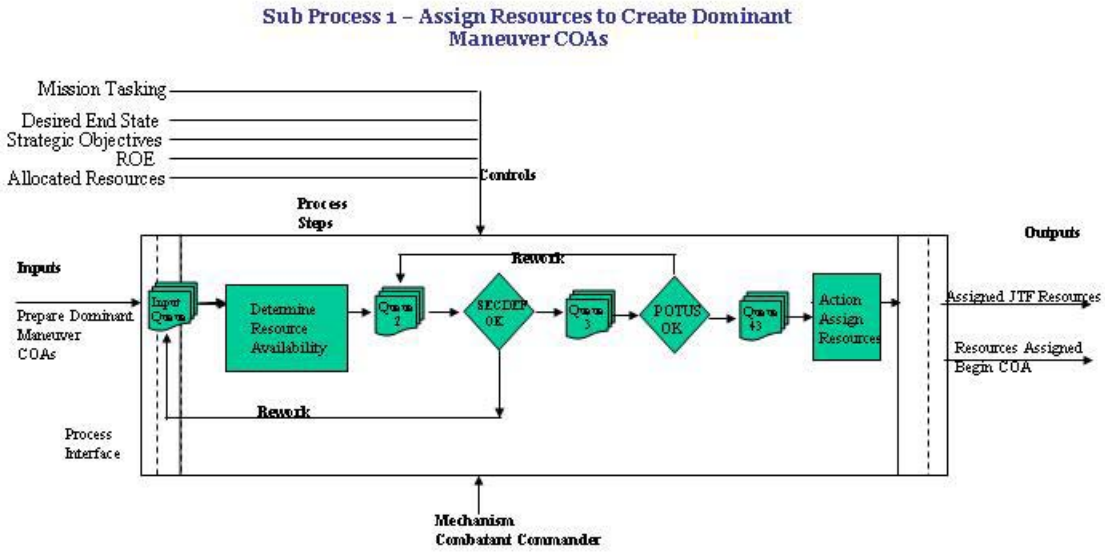


Figure 19 – Assign Mechanisms Process

Activity required: This sub process must allocate the resources necessary for the other two sub processes. The other two sub processes are dependent upon this allocation and thus may not begin until this process has produced its outputs in terms of mechanism/resource availability and suitability to the tasks. For drawing simplicity, all possible inputs and controls are not shown on the primary process diagram.

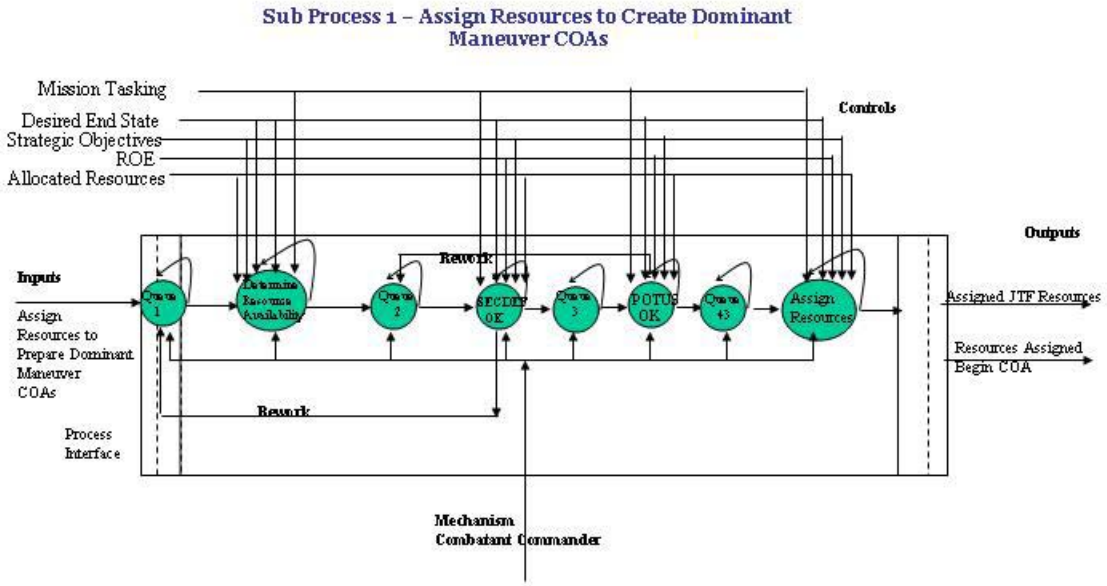


Figure 20 – Assign Mechanisms Process Nodal Model

Controls which must be reflected as components of the output set:

1. **Mission tasking**
2. **Desired End State**
3. **Desired Operation Effects**
4. **ROE – Rules of Engagement**
5. **Strategic Objectives**

Mechanisms

1. **Combatant Commander**

Inputs

1. **Activate Order for New Theater COA Dominant Maneuver**

Approvals

1. **CJTF**
2. **SecDEF**
3. **POTUS**

Outputs

1. **Resource Planning Complete – Start Next Sub Process**
2. **Staff Assignments as dedicated mechanisms to the next sub processes**

Process 1 Scores
Process 1 Node Density = 8

Approval Node Workflows = 2
Process 1 Organizational Reynolds Number = .13757 = Low Process Viscosity and Turbulence Risk

2 rework lines, centralization factor = .8, error probability = .05
OR_N = e/C + 0.25 * Log(D)

ORn = .05/.8 + .25*Log(2) = .0625 + .25(.30103) = .0625 + .137757 = .137757

Process 1 Simulation equations
Node 1
Queue 1 – Input Queue
1. **Arrival Rate = λ**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 2 – Determine Resource Availability
1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 3
Queue 2 – Resource Plan Approval Queue for SecDef
1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 4 – SecDef Evaluates / Approves Resource Assignment Plan
1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 5
Queue 3 – POTUS Resource Plan Approval Queue
1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**

3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Node 6 – POTUS Approval Node

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 7-

Queue 7 – Approve Resource Plan Action Queue

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Node 8 – Resource Assignment Action Node

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Explosion of the Generate COA Options Process

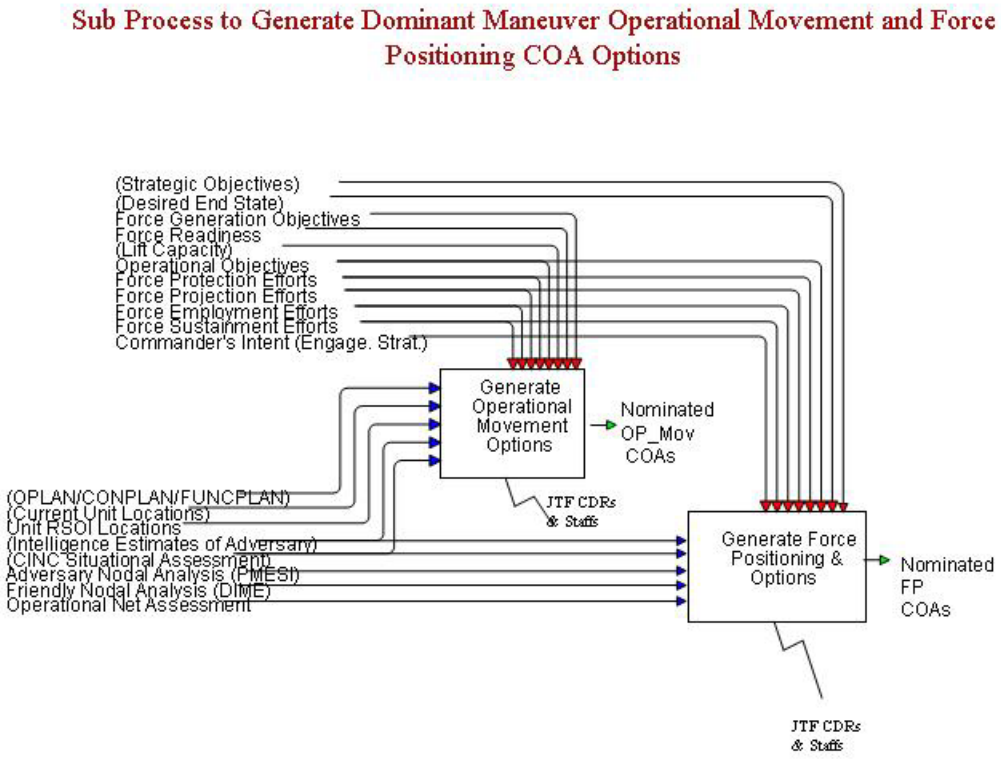


Figure 21 – Process to create COAs

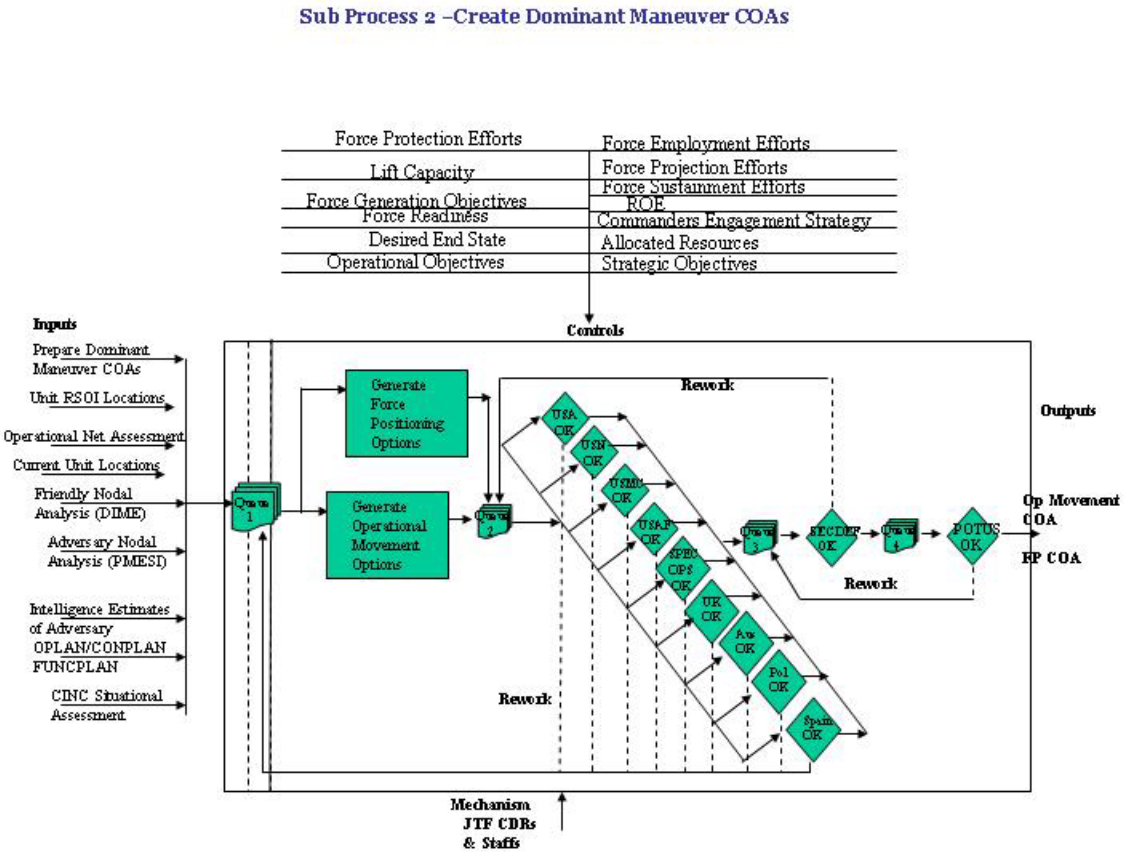


Figure 22 – Create COA Process Model

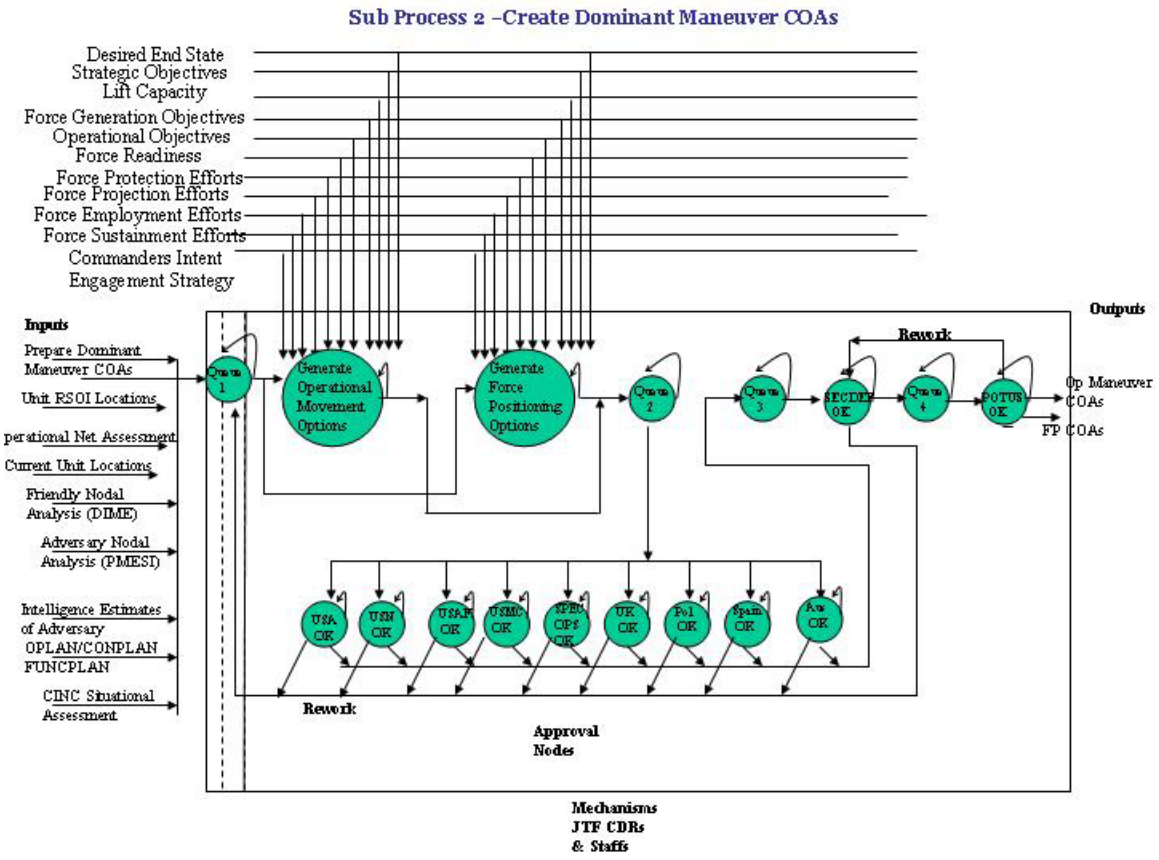


Figure 23– Create COA Process Nodal Model

Controls – Must be sectioned and addressed in output sections of COAs

1. **Strategic Objectives**
2. **Desired End State**
3. **Force Generation Objectives**
4. **Force Lift Capacity**
5. **Operational Objectives**
6. **Force Protection Efforts**
7. **Force Projection Efforts**
8. **Force Employment Efforts**
9. **Force Sustainment Efforts**
10. **Commanders intent engagement strategy**

Mechanisms

1. **JTF Commanders**
2. **General JTF staff**

Inputs

1. **OPLAN/CONPLAN/FUNCPLAN**
2. **Current unit locations**

3. **Unit RSOI Locations**
4. **Intelligence Estimates of Adversary**
5. **CINC Situational Assessment**
6. **Adversary Nodal Analysis (PMESI)**
7. **Friendly Nodal Analysis (DIME)**
8. **Operational Net Assessment**

Approvals

1. **Army FP COA approver**
2. **AF FP COA Approver**
3. **NAVY FP COA Approver**
4. **MC FP COA Approver**
5. **SPEC OPS U.S. COA Approver**
6. **SPEC OPS U.K. COA Approver**
7. **SPEC OPS Poland COA Approver**
8. **SPEC OPS Spain COA Approver**
9. **SPEC OPS Australia COA Approver**
10. **CJTF**
11. **SecDEF**
12. **POTUS final**

Outputs

1. **Nominated Operational Movement Options Courses of Action**
    - i. **Strategic Objectives**
    - ii. **Force Generation Objectives**
    - iii. **Force Lift Capacity**
    - iv. **Operational Objectives**
    - v. **Force Protection Efforts**
    - vi. **Force Projection Efforts**
    - vii. **Force Employment Efforts**
    - viii. **Force Sustainment Efforts**
    - ix. **Commanders intent engagement strategy**
    - x. **Desired End State**

2. **Nominated Force Positioning Options Courses of Action**
    - i. **Strategic Objectives**
    - ii. **Force Generation Objectives**
    - iii. **Force Lift Capacity**
    - iv. **Operational Objectives**
    - v. **Force Protection Efforts**
    - vi. **Force Projection Efforts**
    - vii. **Force Employment Efforts**
    - viii. **Force Sustainment Efforts**
    - ix. **Commanders intent engagement strategy**
    - x. **Desired End State**

Process 2 Scores

Node Density = 17

Process 2 Organizational Reynolds Number = .3125 = Very High Process Viscosity and Turbulence Risk

10 rework lines, centralization factor = .8, error probability = .05
OR_N = e/C + 0.25 * Log(D)

ORn = .05/.8 + .25*Log(10) = .0625 + .25(1) = .0625 + .25 = .3125

Process 2 Simulation equations
Node 1
Queue 1 – Input Queue

1. **Arrival Rate = λ**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 2 – Generate operational maneuver options

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 3 -
Queue 2 – Op maneuver COA Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Nodes 4 -12 Parallel COA Approval Nodes

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 13 – Generate Force Positioning COAs

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 14 -
Queue 3 – Op maneuver COA SecDef Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 15 – SecDef Evaluates / Approves COAs

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 16

Queue 4 – POTUS Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Node 17 – POTUS Approval Node

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Explosion of the sub process to provide commander's estimate

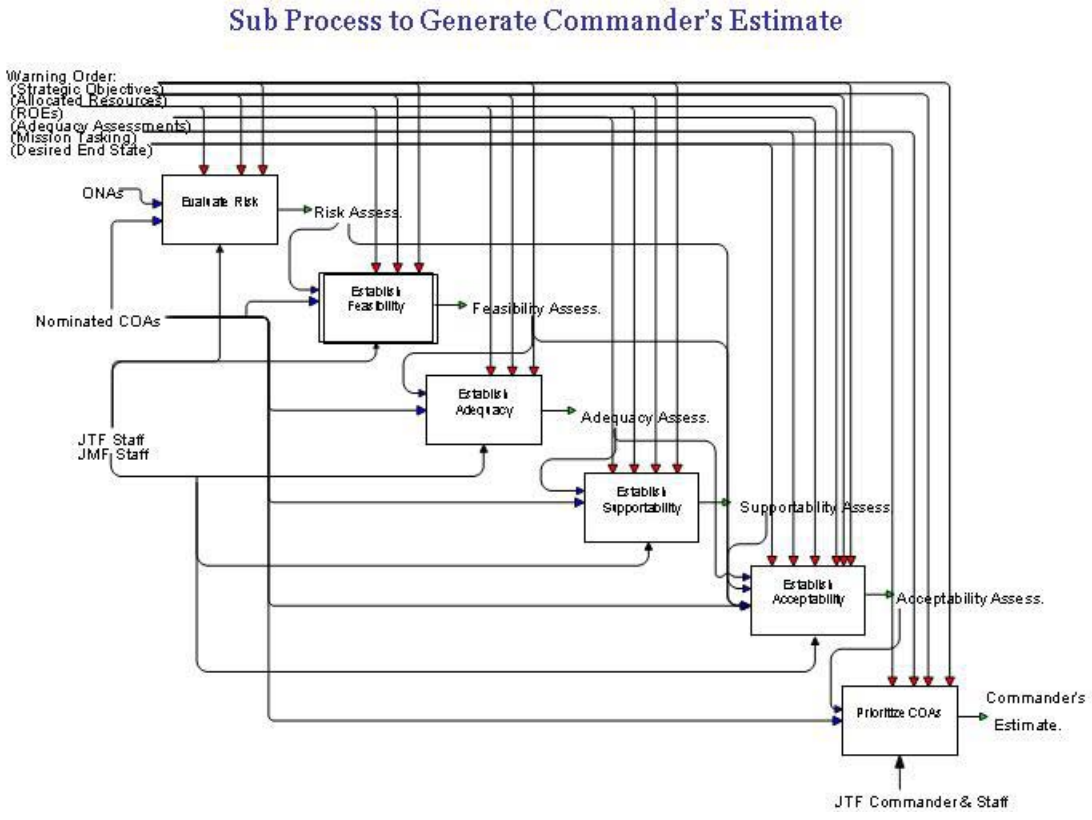


Figure 24 – Create Commander's Estimate Process Model

The following is the state model of the above diagram

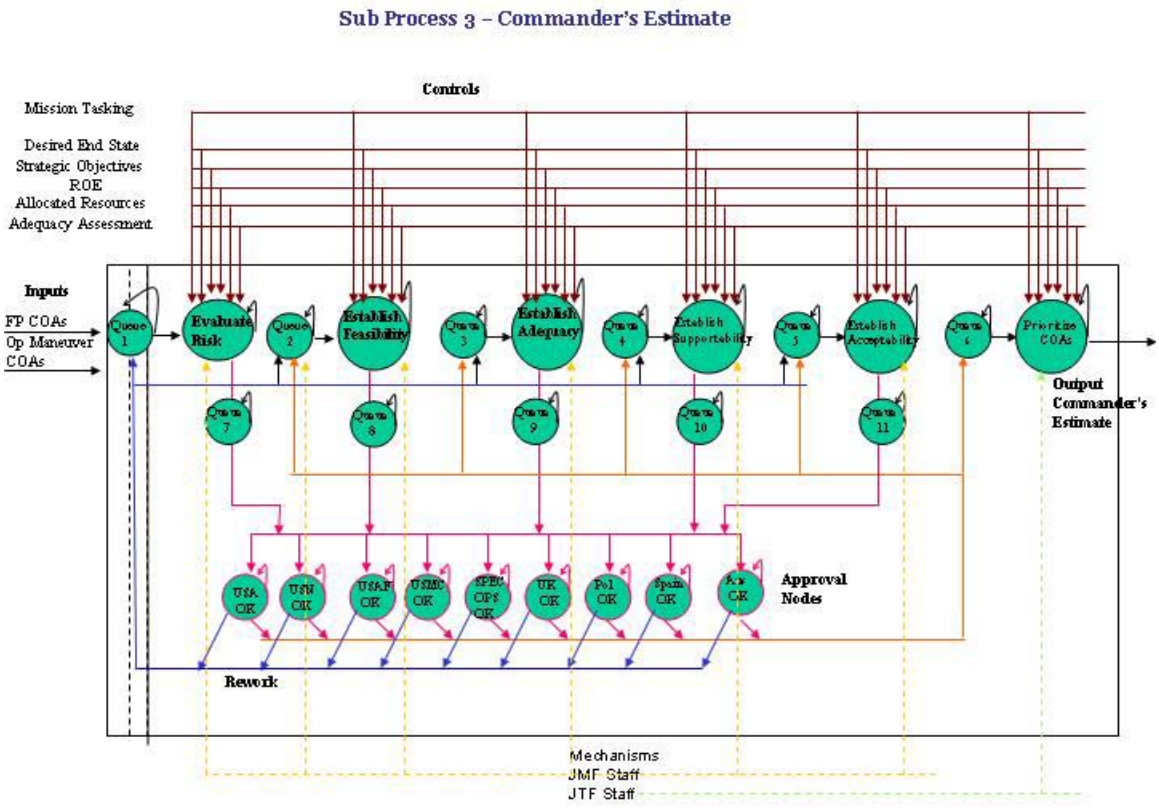


Figure 25 – State model of Commander's Estimate Process

Controls

1. **Strategic Objectives**
2. **Allocated Resources**
3. **Rules of Engagement – ROE**
4. **Desired End State**
5. **Adequacy Assessment**
6. **Mission Tasking**

Mechanisms

1. **JTF Commanders**
2. **General JTF staff**

Inputs

1. **Nominated COAs**
2. **ONA**

Approvals

1. **Army Commanders Estimate Approver**
2. **AF Commanders Estimate Approver**
3. **NAVY Commanders Estimate Approver**
4. **MC Commanders Estimate Approver**
5. **SPEC OPS Commanders Estimate Approver**
6. **SPEC OPS Commanders Estimate Approver**
7. **SPEC OPS Poland Commanders Estimate Approver**
8. **SPEC OPS Spain Commanders Estimate Approver**
9. **SPEC OPS Australia Commanders Estimate Approver**
10. **CJTF –**
11. **SecDEF**
12. **POTUS final**

Outputs

1. **Risk Assessment**
2. **Feasibility Assessment**
3. **Adequacy Assessment**
4. **Supportability Assessment**
5. **Acceptability Assessment**
6. **Commanders Estimate**

Process 3 Scores

Node Density = 26

Process 3 Organizational Reynolds Number = .301 Very High Process Viscosity and Turbulence Risk

Rework lines = 9, centralization factor = .8, error probability = .05
OR_N = e/C + 0.25 * Log(D)

ORn = .05/.8 + .25*Log(9) = .0625 + .25(.9542) = .0625 + .238 = .301

Process 3 Simulation equations
Node 1
Queue 1 – Input Queue

1. **Arrival Rate = λ**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 2 – Evaluate Risk

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 3 -
Queue 7 – Risk Plan Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Nodes 4 -12 Parallel Risk Approval Nodes

1. **Arrival Rate = λ = Completion rate of Node 2**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = MAX(nodes 4- 12) ($W = \lambda X^2 / 2(1-p)$)**

Node 13
Queue 2 – Feasibility Queue

1. **Arrival Rate = λ = Completion rate of Nodes 4-12**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Node 14
Establish Feasibility

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 15
Queue 8 - Establish Feasibility Approvals Queue

1. **Arrival Rate = λ = Completion rate of Node 14**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 / 2(1-p)$**

Nodes 4 -12 Parallel Feasibility Approval Nodes – for node 14 work approvals

1. **Arrival Rate = λ = Completion rate of Node 14**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = MAX(nodes 4- 12) ($W = \lambda X^2 / 2(1-p)$)**

Node 16
Queue 3 – Establish Adequacy Queue

1. **Arrival Rate = λ = Completion rate of Nodes 4-12**

2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 17
Establish Adequacy

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 18
Queue 9 Adequacy Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 17**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Nodes 4 -12 Parallel Adequacy Approval Nodes – for node 14 work approvals

1. **Arrival Rate = λ = Completion rate of Node 18**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = MAX(nodes 4- 12) ($W = \lambda X^2 /2(1-p)$)**

Node 19
Queue 4 – Establish Supportability Queue

1. **Arrival Rate = λ = Completion rate of Nodes 4-12**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 20
Establish Supportability

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 21
Queue 10 Supportability Approval Queue

1. **Arrival Rate = λ = Completion rate of Node 20**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Nodes 4 -12 Parallel Adequacy Approval Nodes – for node 20 work approvals

1. **Arrival Rate = λ = Completion rate of Node 20**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = MAX(nodes 4- 12) ($W = \lambda X^2 /2(1-p)$)**

Node 22
Queue 7 Acceptability Queue

1. **Arrival Rate = λ = Completion rate of Nodes 4-12**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 23
Establish Acceptability

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Node 24
Queue 11 acceptability Approval Queue
Acceptability Queue

1. **Arrival Rate = λ = Completion rate of Node 23**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Nodes 4 -12 Parallel Acceptability Approval Nodes – for node 20 work approvals

1. **Arrival Rate = λ = Completion rate of Node 23**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = MAX(nodes 4- 12) ($W = \lambda X^2 /2(1-p)$)**

Node 25
Queue 6 Prioritize COA & Create Commander's Estimate Queue

1. **Arrival Rate = λ = Completion rate of Nodes 4-12**
2. **Content = Number of Inputs at Time (T) – Number of Service Completions by Time (T)**
3. **Wait time = Mechanism Availability Latency + Average Queue Wait Time = $W = \lambda X^2 /2(1-p)$**

Node 26
Prioritize COA & Create Commander's Estimate

1. **Processing Time = Analysis Latency + Data Latency + Decision Latency + Rework Time + Mechanism Latency**

Process 3 Time $T_{(P3)} = \sum T_{(Node\ 1)} + T_{(Node\ 2)} \ldots T_{(Node\ 26)}$

Process configuration differences
Serial Model Total Process Time = $\sum T_{(P1)} + T_{(P2)} + T_{(P3)}$
Parallel Model Total Process Time = $T_{(P1)} + MAX(T_{(P2)}, T_{(P3)})$

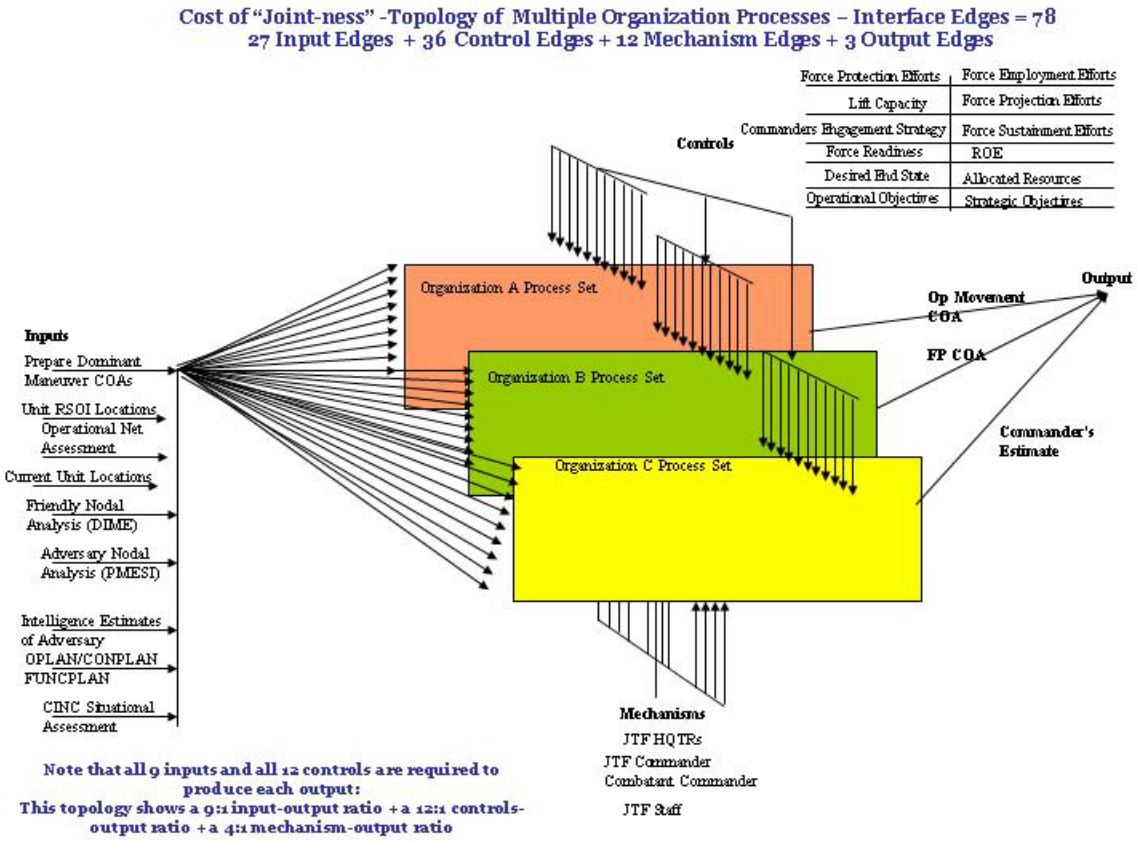


Figure 26 – Dominant Maneuver Processes in Multiple Organizations Topological View

Process Interface Topology Metrics Discussions

The above topological view of the test model depicts several important issues. Adding a process in parallel in the form of multiple organizations may bring more resources to bear on the input to be processed, however, it may also increase the complexity and latencies of inter-process synchronization.

Input latencies are increased by definition
Dissemination Latency = high

Interface adaptation or realignment latency = high since interfaces may not be interoperable.
Process adaptation latency = high due to number of approval nodes and controls
Node adaptability latency or realignment latency
Queue adaptability or realignment latency
Mechanism adaptation latency or mechanism realignment latency - high latency due to multiple organizations requiring similar mechanisms
Controls realignment latency or rules adaptation latency – high latency due to multiple organizations adapting to new controls
Adaptability may be severely lessened unless the process re-alignment plan is designed to compensate for such training and understanding deficiencies

Approval Workflow Model – provided as information only to depict possible workflow and approval steps

The approval chain depicted in the graphic below will be used in the appropriate processes and sub processes. Only the chains of command that depict various concepts described above in terms of approval centralization will be selected. This should assist the reader in identifying how approval or decision centralization bottlenecks contribute to a high Organizational Reynolds Number.

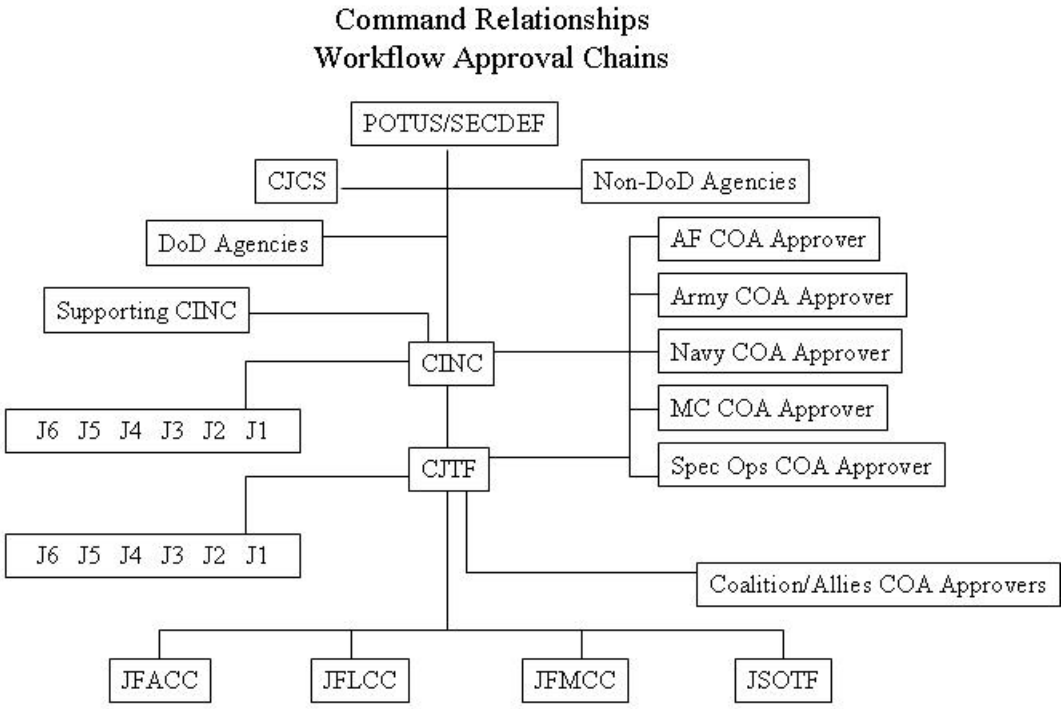


Figure 27 – Notional Workflow Approval Chains

A Description of the Unified Command Structure Model

The model below represents the framework at a simple level. The basic model reflects a standard IDEF structure in terms of inputs, outputs, constraints, and resources.

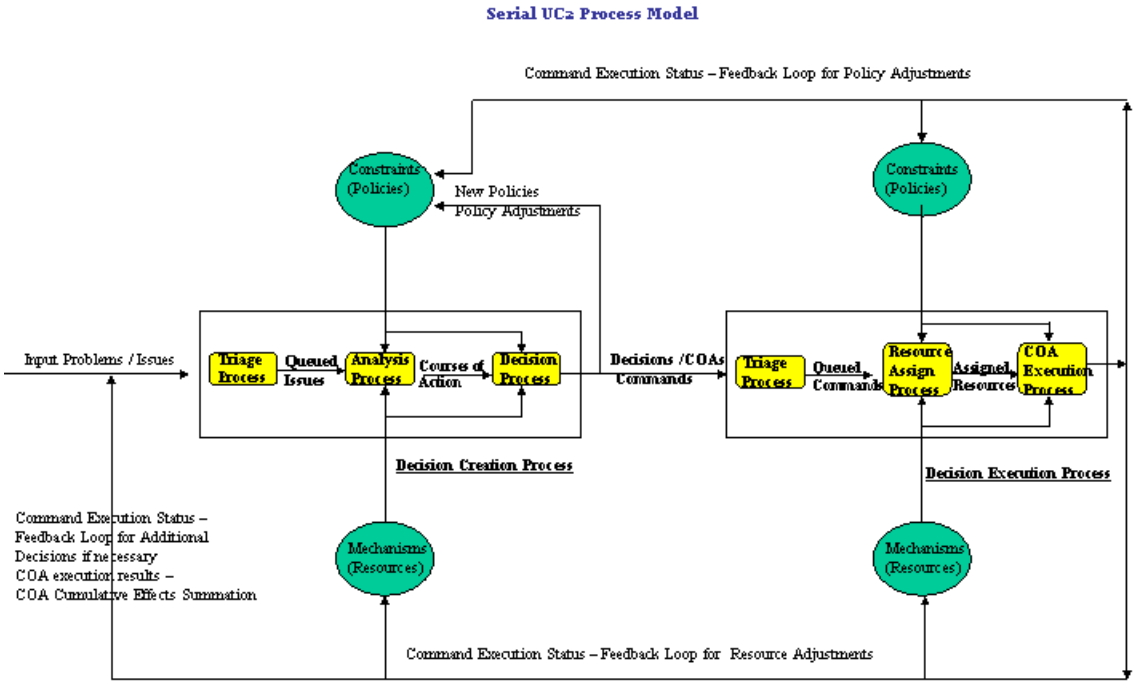


Figure 28 - Simple Serial UCS Process Model

The simple serial model is composed of two major processes, a Decision and Policy Creation Process, and a Decision Execution Process.

The Policy and COA Creation Process Model operates in two modes: decision creation mode or policy generation mode. In **COA creation mode**, inputs are received and prioritized for analysis (triaged). The analyst evaluates the highest priority problem in his input queue and creates a course of action and a set of alternative courses of action. The analyst is constrained in his preparation by constraints from prior existing policies and resource availability. The COAs are presented to the decision maker who selects the most appropriate COA from the set of alternative COAs. The outputs are COAs or commands.

In **policy generation mode**, the analyst has no high priority problems assigned, and instead is assigned to create policies for proactive management of the set of highest probability potential problems. Again, the analyst is constrained in his preparation by constraints from prior existing policies and resource availability. The analyst presents the new or innovative proactive policies to the decision maker who approves or modifies the newly created policy for addition to the policy store. The outputs are new or modified policies.

The Decision Execution Process Model receives its input from the decision creation model as courses of action, commands, or policies to be implemented. Inputs are assigned priorities, then processes and virtual organizations are created, execution plans are

generated, tasks and resources are assigned and staged, training is implemented, and the plan is executed. Command execution status is the output generated and fed back to the decision creation process as input.

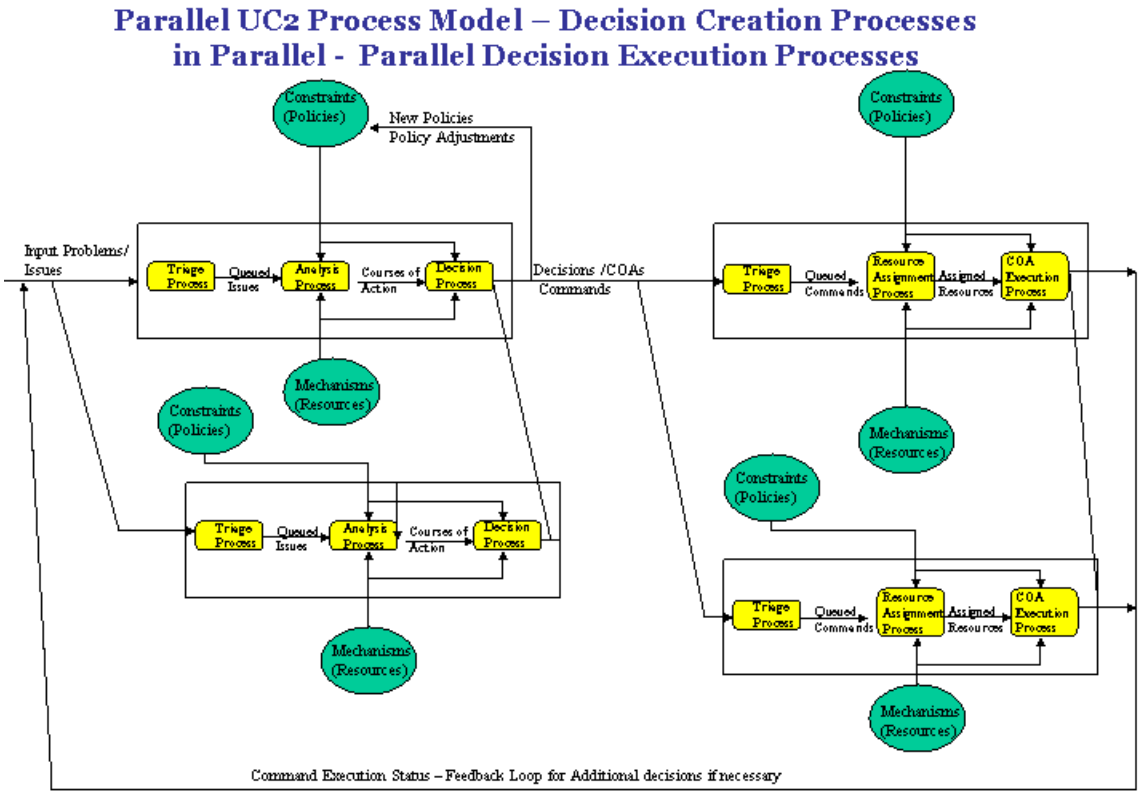


Figure 29 - UC2 Parallel Process Model

The Parallel UC2 Process Model behaves similarly to the serial model with the key difference being the introduction of concurrent, synchronized decision creation and synchronized decision execution processes. Parallel processing offers the opportunity to decompose problems for analysis and creation of courses of action in such a way as to permit simultaneous work to occur on the same problem or policy. The instantiation of the organizations required to achieve parallelism may be from agreements between existing organizations or by the instantiation of temporary "virtual" organizations with resources shared between lending organizations. While figure 29 only depicts 2 parallel sets of processes, in reality, "N" parallel processes may exist and be synchronized or un-synchronized. By synchronized processes, I mean that, at any given time, the joined "clone" or shadow processes are working to achieve the same objectives and to solve the same original problem set. Referencing figure 29's decision creation processes above, please note that this synchronization only has meaning with respect to shared similar activities. Thus, the triage problem prioritization processes must be shared and synchronized, the problem analysis processes must be processes must be shared and synchronized, and the decision making process must be shared and synchronized in order

for the entire set of Decision Creation Processes to be synchronized. The same would be true of the decision execution processes. In my opinion, parallel processes also introduce process management complexities. It is of particular importance that Service Level Agreements be embedded in the processes, with their corresponding QoS clauses, in order to simplify the execution and instantiation of multiple parallel processes. The SLA between the resource providing agencies should refer to lexicon segments appropriate to binding resources to virtual organizations.

How to use the shared process interface models

The process models should be viewed as a closed system. This enables many features to be considered in their proper context. I have assumed for purposes of this discussion that an adversarial use of the model is necessary. The models should be used as a tool to evaluate "real world" scenarios. The scores of the scenarios can be compared against various instantiations of the abstract model hopefully identifying weaknesses in processes, tools, and polices.

First, for a given problem or issue, the model must have a desired outcome. The outcome may be defined in the form of game theoretic terminology as a starting point. The figure below depicts the possible outcomes of a shared outcome version of the model, meaning that adversaries share the outcome of their respective processes. The model user must decide for any given set of commands, policies, or solutions what the anticipated outcome will cost. If the user of the model wishes to maintain a "status quo" (for example, the Cold War), then the policies and courses of action chosen should be designed to create a zero sum output.

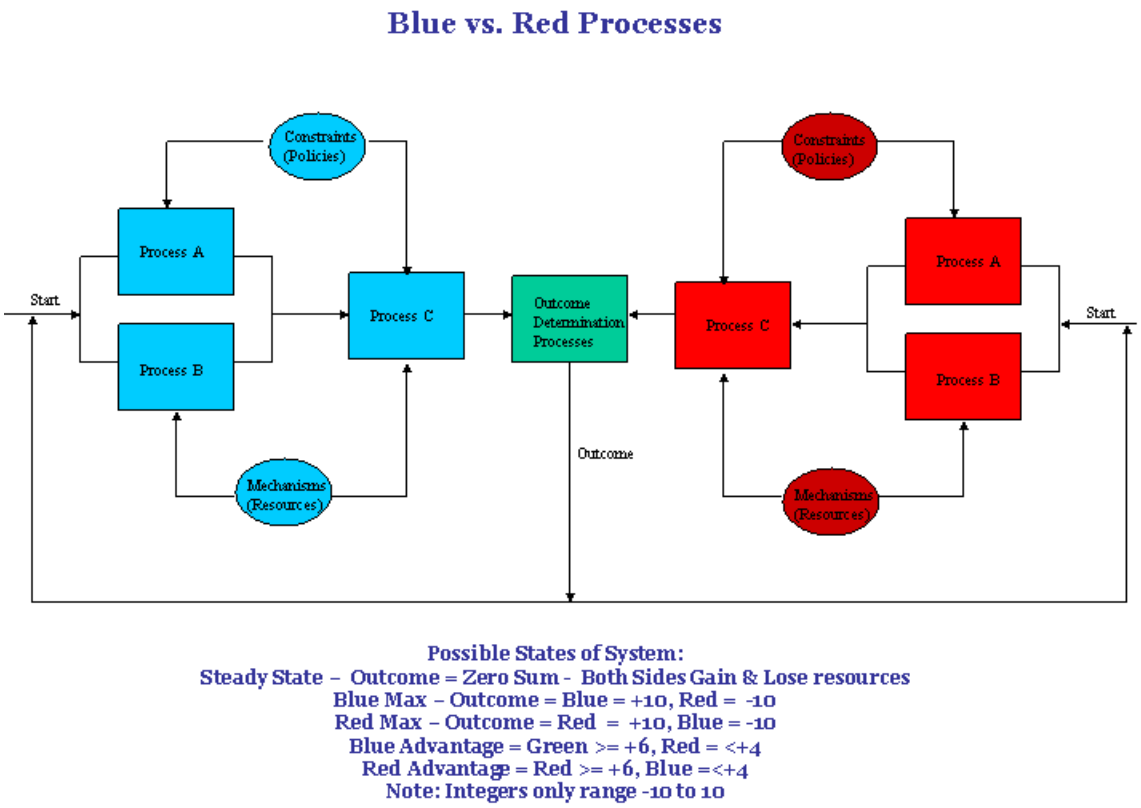


Figure 30 – Shared Outcome Process Model

If the model user wishes to defeat an adversary totally, then a min-max version of policies should be designed. Once the goals of the process are understood, then the user can select which problem to address first through the triage process previously defined above. The analyst is the next model user. The analyst takes his work from the triage queue by highest assigned priority and using the vector dimensions of the problem, determines the complexity of the problem. The analyst must also determine if the problem is clearly understood, and if all the data necessary for a good decision selection is readily available. The time required to capture the data is called data latency. See figure below, (Note that this material is from the work published by Richard Hackerthorn, "Factors for Implementing Active Data Warehousing", 7/28/2003, available at datawarehouse.com) If the problem is very complex, after problem decomposition, the analyst may wish to establish multiple parallel analysis processes. This should not be performed in haste as it may actually slow down the decision process, which matters in the case of time critical problems. The time required by the analysts to create the set of courses of action and alternative courses of action is called analysis latency. Adding or subtracting processes and analysis organizations may adversely impact analysis latency and should thus be evaluated prior to instantiating more blue analysis teams.

How to use the metrics

Simply put, the metrics defined in this paper should be used as qualifying criteria in the evaluation of any system or process being considered in the C2 domain. Does the proposed C2 enhancement process or technology enhancement reduce data latency, analysis latency, decision latency, or action distance? Are inputs dimensions more manageable? Can the new system reduce the volume or frequency of issues? Can the truth value be easily determined? Is the ability to quickly map problems to known successful COAs or policies enhanced? Are the belief systems or Memetics easily captured? Are process workflow automations enhanced? Is the common lexicon enhanced or made richer to enable shared understanding? Are service level agreements and quality of service implementations facilitated? Is the ability to identify problem and solution inter-relatedness enhanced? Is the ability to provide a sigmoid feedback analysis enhanced for managing effects based operations? Is the use of a UC2XML being expanded to support automated process self-learning tools? Are process costs and COA execution costs being properly captured in order to refine resource expenditure? Are tools needed for robust inter-agency resource mapping available?

Proposed process and mechanism evaluation process to influence procurement

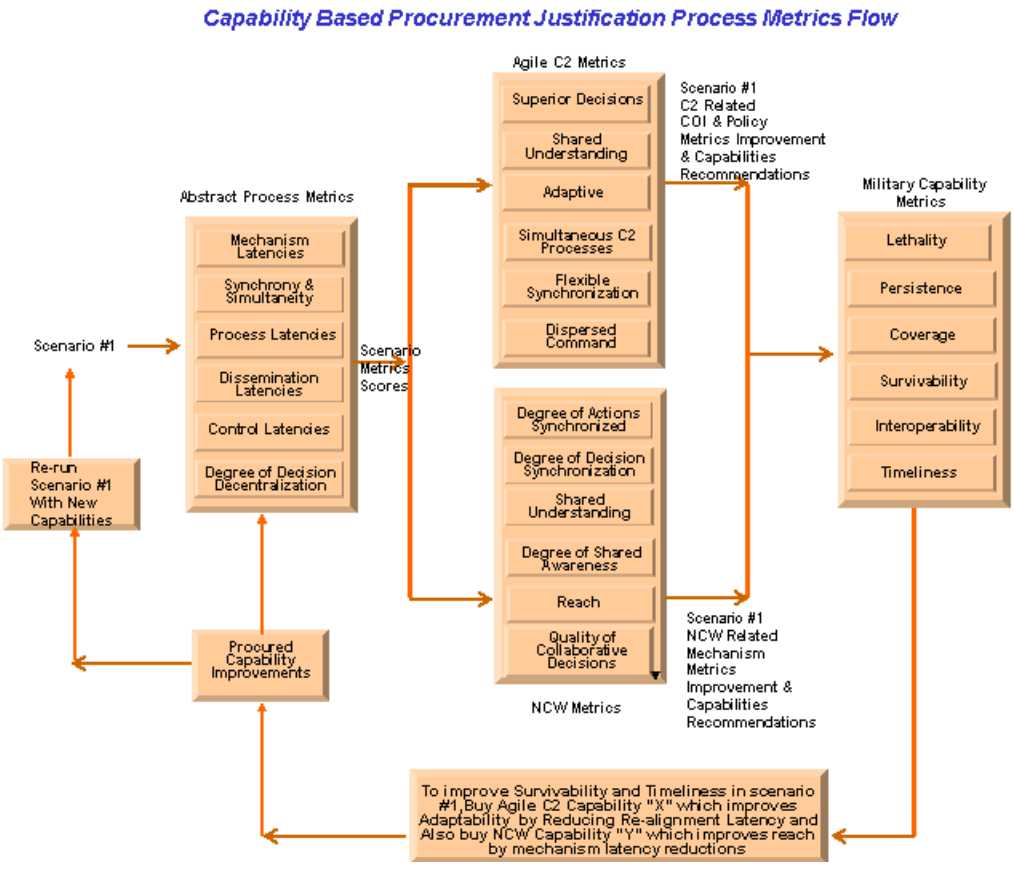


Figure 31 – Process Assessment Process Model

The diagram above depicts the process suggested to exploit the metrics and analyses in this paper.

1. Take a given scenario and convert the steps in the scenario into "process centric" and abstract steps to the greatest extent possible. Do not use system names, network references, etc. Only process terms such as inputs, controls, rules, nodes, and mechanisms.
2. Apply the required formulas from the abstract model and create the process centric workflows.
3. Evaluate the process steps and determine the first run metric values. This is baseline 1. The abstract baseline.
4. Perform process optimization, resource optimization, control/rule optimization.
5. Re-evaluate the metrics (re-compute the formulas / equations) and repeat process optimization steps until you are sure that all process latencies have been reduced or eliminated. This is baseline 2 – The optimized process baseline.
6. Replace the abstract mechanisms with existing resources and systems and re-baseline the equations. This is baseline 3 – systems based baseline
7. Identify mechanisms that could reduce latencies if they existed. These mechanisms are "gaps". Re-run the baseline and validate that the proposed gap solutions (new mechanisms) actually show latency reductions. This is the to-be baseline.
8. Perform financial simulation and procure if justified.
9. Re-run baseline with newly procured "gap solution" mechanisms and validate the entire process.

Appendix I - Map of Abstract Process Metrics to Agile C2 Metrics

Note that these metrics relationships are only valid after the abstract process has been extracted from a scenario and that the latencies and ORn, etc. for each organization's process set have been determined.

Attributes of Agile C2

Superior Decision Making, If a decision achieves its objectives within time boundaries proscribed in the COA or policy controls, and according to the accepted COA within the desired mechanism expenditures without violating the controls then it should be considered a superior decision. Thus, mechanism expenditure count and objective achievement count during the achievement time window for a COA should be the primary measures. Example, Deployed 100,000 members of Armed forces, destroyed all 5000 targets in 1 week, at a casualty count of 0, equipment loss of 0, and a collateral damage count of 0. Less superior decisions would indicate mechanism losses greater than 0, or target objectives count less than optimum, or time constraints exceeded, or ROE violations counts.

Flexible Synchronization, latency metrics for controls changes (control re-alignment latency) and mechanism re-alignment latency given a new task. In other words, the process or its mechanisms are more flexible for synchronization if the process control rules are not in the way or there is not a large centralization factor, or if the resources are not going to require new training.

Simultaneous C2 Processes, Number of Topology edges in multiple processes or organizations which are concurrently active for the same queue entry and share the same control set

Dispersed Command, Low centralization score = dispersed command, decisions made locally, the higher the centralization of decisions, the less dispersed the command. An interesting issue with this metric occurred in the Serbian conflict. Local commanders were required to have their plans reviewed at a higher level (higher centralization metric) after the targeting tragedy at the Belgrade Embassy of the People's Republic of China. So if dispersed command actually exists, un-managed inputs can force a change in controls and centralization effectively dismantling dispersed command.
Nodal Viscosity & missing truth content (no SVT) caused the un-managed input to occur forcing the process change, thus this is a fluid metric depending upon unanticipated effects

Shared Understanding, Refers to active process task resources ability to understand controls and task details. This metric is represented by the following counts: Number of perfect cognates in common lexicon for shared rule set (controls), shared input meme count, and shared COA data sets. Also, this metric can be countable or measurable by low mechanism re-alignment latency.

Responsive, Processes containing low nodal viscosities, low action distance scores and low Organizational Reynolds numbers are responsive. Value of Process Efficiency as reflected in high data latency or analysis latency = poor responsiveness, high Organizational Reynolds Number (>.25) = poor responsiveness, high nodal viscosity due to multiple versions of the truth also = poor responsiveness.

Tailorable, Processes with low dissemination latency, low Organizational Reynolds Number scores, low centralization, and low resource re-alignment latency are said to be tailorable.

Integration of C2 components, The degree of difficulty of process merging as measured by the number of topology edges, dissemination latency, controls latency, nodal viscosity, mechanism re-alignment latency, inconsistent levels of decision centralization, lack of well defined lexicon, poor shared understanding, and the absence of well defined SOAs and QoS agreements. Thus, processes with high latency scores, high degrees of centralization of decision making, no or poor lexicons, and high numbers of topological edges will be difficult to integrate. This metric should become a checklist as listed.

Agile C2 Properties and Attributes to Abstract Process Metrics Entity Relationships

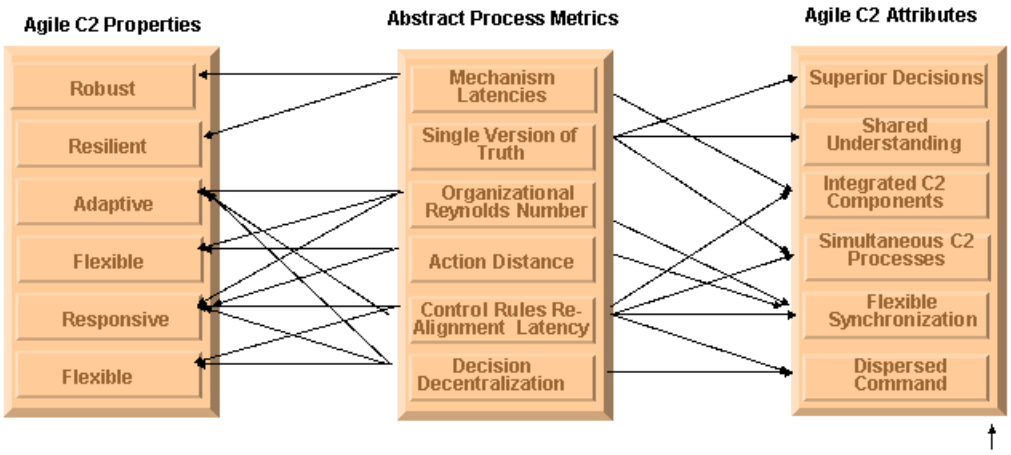


Figure 32 – Metrics Class Relationships

The figure above is provided as a tentative map of a subset of the Agile C2 attributes and properties to the abstract process metrics defined in this paper. The research in this paper appears to indicate that a many to many relationship exists between the metric entities. Further analysis is required to determine if these relationships can be simplified.

Appendix II - Map of Abstract Process Metrics to Agile C2 Properties

Robust – strength against disasters, A process or process mechanism Disaster Recovery system used in conjunction with the resilience mechanism to help ensure high availability. Usually accomplished by providing geographically disbursed "mirrored" resource. These mirrors can assume full mechanism capability delivery in the case of a disaster (natural or military) to the primary mechanisms. Usually contains the same SLA/QoS as the resilience metrics. See discussion below. A process or process

mechanism is robust if it can seamlessly be transitioned in the case of disasters. Process or mechanism users experience no to minimum loss of process or mechanisms. Measured the same as resilience. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Robustness: the ability to maintain effectiveness across a range of tasks, situations, and conditions***

Resilient ***(Availability),*** A process mechanism redundancy metric which defines the percent of High Availability or Survivability due to a loss of a particular resource. The time a process or a process mechanism is unavailable while operating in a given scenario. Usually refers to the so called "5 nines" availability metric. For example, a computer system used as a mechanism which operates under an SLA of "5 nines", has a QoS requirement of being available and useable 99.999% of the time 24 hr per day, seven days a week, for one year. Thus, for the total hours in a year of 8760, a maximum down time of 8.76 hrs in the year or .024 hrs per day or 1.44 minutes loss of daily mechanism use is permitted, exceeding 1.44 minutes of mechanism or process usability a day, violates the quality of service metric for this service level agreement.
Resilient processes by definition are designed to meet this metric. The percent in excess of 1.44 minutes per day of unavailability or loss of usability measures the loss of resilience. For mechanism availability, this almost always implies highly available, automated fail over systems. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Resilience: the ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the Environment.***

Responsive (Per Design), is measured in terms of SLA/QoS process throughput times being met. For example, if a process SLA requires that any input be processed error free in terms of time, and the process produces the output within the time constraints, then the process is responsive against a design. When the process time exceeds the SLA/QoS requirements, then the amount of time over the QoS expressed as a percent of overtime is the measured metric.

Responsive (Process re-configurability), means that a process can be used to process a new type of input or similar inputs with minimal process or mechanism changes. The primary metrics for this are mechanism realignment latency or controls realignment latency. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Responsiveness: the ability to react to a change in the environment in a timely manner.***

Flexible (Scenario independence), the number of scenario input type varieties that can occur without changing mechanisms or controls. The number of unique process outputs that can be generated by the same control set, node set, and mechanisms sets given a variety of input types. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Flexibility: the ability to employ multiple ways to succeed and the capacity to move seamlessly between them.***

Innovative, Low process control set rigidity metric – low centralization factor and flexible span of control. Controls permit mechanisms to develop novel solutions to

process input variations – Processes with low controls realignment latencies and low centralization scores can be innovative. Processes with absolutist controls (no rule changes without approval) are not likely to support innovation. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Innovation: the ability to do new things and the ability to do old things in new ways.***

Adaptive, Measured by low process latencies, low Organizational Reynolds Number scores and low organizational centralization scores. Organizations capable of quickly instantiating a VIMO with a well defined SLA/QoS epitomize process adaptability. Processes, nodes, controls, and mechanisms are all measurable for adaptive-ness scoring. Processes with high node density are not adaptive, the lower the node density the higher the adaptability, the lower the Organizational Reynolds Number the higher the adaptability of the process, the higher the diversity of the mechanism set members' skills the higher the process adaptability. By definition, network centric mechanisms are more adaptive since the mechanisms have a rapid access to data (low data latency), less dissemination latency in the case of a VIMO, and permit the configuration of composeable functions which create newer capabilities faster than traditional system installation. Again by definition, processes containing NCW mechanisms are more adaptive because they benefit from high reach and high degrees of networking. Compare to [18] the definitions offered by Alberts and Hayes in their work Power to the Edge: ***Adaptation: the ability to change work processes and the ability to change the organization.***

Appendix III - Map of Abstract Process Metrics to Network Centric Warfare Metrics

Please note that all of these metrics are related only to the mechanism aspects of a given process or set of processes. In other words these metrics are mechanism valid only.

Degree of networking is the number of nodes in a specific process during a specific scenario, which contains mechanisms capable of accessing or utilizing the same resources or services of a WAP, LAN/WAN Intranet, Extranet, or the Internet. Thus, if a process contains 10 nodes, and only 5 nodes have service network access, then the degree of networking is 50%.

Reach is a similar metric referring to the number of nodes covered by the same network mechanism in a given process set. For complex process topologies, the process set must be defined in order to define the degree of networking. For example, if a parallel process set contains three processes owned by 3 different organizations, of which 2 processes have networks and one does not, then the reach in terms of network access is 2/3 or 66%. However, there is a special case where if the nodal resources are on an intranet or secure network but the other process nodal resources cannot access the same mechanisms in the same specific process, then the reach for that process for a given scenario is zero for the case in which all nodes are networked but on different secure networks**.**

Network Assurance refers to the ability of a network mechanism to be available and useable for a given set of nodes in a specific process during the execution a specific scenario. This is usually measured as part of a Service Level Agreement and Quality of

service metric for the particular resource. In the case of networks, this must include high availability (usually to "5 nines", see discussion above concerning resilience), and disaster recovery, see discussion above concerning robustness, and information operations protection of the network mechanisms from denial of service attacks, intrusions, and data degradation.

High Network Assurance:

1. 0 data loss or corruptions due to adversarial info ops attacks
2. 0 denial of service attacks
3. 0 intrusions
4. 0 hours of loss of use (high availability and disaster recoverable)

Medium Network Assurance or Meeting Minimum SLA/QoS Standards

1. % greater than 0 of data loss or network data corruptions
2. Number greater than 0 of denial of service attacks
3. Number of intrusions greater than 0
4. Number of hours of loss of use

Poor Network Assurance is any violation SLA/QoS Agreements or Standards for a given process or a process node

Network Agility refers to the mechanism re-alignment latency time for this particular network mechanism in a given process. Can the network be used in a new scenario to support voice, video, chats etc.? If not, how much time will any required adjustments take so that the new network configuration can support say a chat room.

Node Capacity is the number of process threads (individual tasks dispatched from a process queue) that can be handled without exceeding the average task error rates. This needs to be validated per process per scenario. Start by using Poisson distribution and baseline the error rates for regular arrival rates. Then re-run the scenario but randomly vary input characteristics to determine break points of node under examination.

Node assurance refers to the ability of a nodal mechanism to be available and useable for a given set of nodes in a specific process during the execution a specific scenario without suffering degrading information operations attacks. This is usually measured as part of a Service Level Agreement and Quality of service metric for the particular resource. In the case of computer nodes (clients, servers, mainframes), this must include high availability (usually to "5 nines", see discussion above concerning resilience), and disaster recovery, see discussion above concerning robustness.

High Node Assurance:

1. 0 hours of nodal data corruption - bank account hacker money movers for example
2. 0 denial of service attacks – node processes overloading (UNIX for example)
3. 0 account security intrusions
4. 0 hours of loss of use (high availability and disaster recoverable)

Medium Node Assurance or Meeting Minimum SLA/QoS Standards

1. % greater than 0 of data corruptions - bank account hacker money movers for example
2. Number greater than 0 of denial of service attacks - node processes overloading (UNIX for example)
3. Number of intrusions greater than 0
4. Number of hours of loss of use

Poor Nodal Assurance is any violation SLA/QoS Agreements or Standards for a given process or a process node.

Synchrony or Degree of Actions Synchronized is the number of nodes and mechanisms in "N" processes actively working on the same task. The metric for this is the synchrony metric.

Degree of Effectiveness is the number of objectives identified in the COA or policy for a specific process which have been achieved divided by the number which could have been achieved. This metric can also be used with a temporal metric to give the degree of effectiveness over time. For example, a COA contained 10 objectives. All ten objectives had to be achieved in 10 hours. If 9 objectives were achieved in the 10 hour window, then the process and its mechanisms were 90% effective.

Degree of Information Shareability is the number of nodes in a set of processes which have access to the same data for a given task.

Degree of Shared Information is the number of mechanisms in a given process set which actually access and use the available information for the synchronized tasks.

Appendix III-A Comments by Dr. Raymond Paul Concerning Agile C2 metrics and processes [21]

The Agile C2 elements focus on the sharing of information and understanding and the collaborative activities which support the continual coordination of multiple decisions in a rapidly evolving battlespace. They also include tools, techniques and procedures to allow commanders to more easily interpret and understanding complex information about the operational environment and communicating that understanding across echelons and functions. Additionally, the elements focus on the dynamic restructuring of organizations and processes across the globe to meet the needs of adapting to changes in the operational environment. This includes the development of fluid Communities Of Interest (COIs) and virtual teams that address specific tasks arising in the course of the operation. They can be drawn from joint, interagency coalition or multinational entities from across the globe. Finally, the elements focus on exploiting information technology including the development of a collaborative information environment and data management framework that support decision making in a dynamic operational environment. By adopting a set of collaborative information environment standards, it is possible to connect all of the basic C2 process loops in their respective organizations.

In order to measure the effectiveness of Unified C2, it is necessary to develop a set of metrics that provide an ability to assess the different attributes of the C2 system and their impact on mission effectiveness. The first step in developing metrics is to identify the important qualities of each attribute. These qualities are called measures. Metrics, which are a standard of measurement, are then used in combination with the measures to evaluate the attributes. The table below depicts a sample of the measures and metrics for Unified C2.

The primary source of metrics is the set of metrics being developed as part of a collaborative undertaking between the Office of the ASD (NII) and the Office of Force Transformation. Together they are leading an effort to develop the Network Centric Operations Conceptual Framework (NCO CF).

Table 4.1 - Agile C2 Elements Definitions

Domain	Attribute	Definition
Cognitive	Superior Decision Making	Leadership and supporting capability to generate alternative actions, identify selection criteria, and assess alternatives to decisively control operational situations. Includes the use of automation in exchange, fusion and understanding of information relevant to rapid collaborated, knowledge-based decision making.
	Shared Understanding	Common appreciation of the situation supported by common information to enable rapid collaborative joint engagement, maneuver and support.
	Flexible Synchronization	Discretion to execute a range of control mechanisms, including self-synchronization, to achieve the commander's intent.
Organizational	Simultaneous C2 Processes	Capability for parallel C2 processes for monitoring and understanding the operating environment and synchronizing actions of assigned forces.
	Dispersed Command and Control	Discretion to disperse Joint C2 elements anywhere without loss of effectiveness to meet mission requirements.
	Responsive & Tailorable Organizations	Proficient, cohesive, task-organized, and networked teams using common procedures, and relevant information capable of responding to rapidly to plan and execute a broad range of military operations.
	Full Spectrum Integration	Effectively incorporates service, interagency and multinational partners into a unified force across echelon, mission and geographic boundaries. The goal of this integration is to harmonize all elements of national power.
Technical	Shared Quality Information	High quality information (information that is relevant, accurate, current, complete, etc.) shared among C2 elements via a robust network that enables shared understanding.

Table 4.2 - C2 Attributes with Sample Measures and Metrics

Attributes	Sample Measures	Sample Metrics
Superior Decision Making	Appropriateness of the Decision	Extent to which a decision is consistent with higher commander's intent
	Timeliness of the Decision	Extent to which currency of a decision is appropriate to the mission
Shared Understanding	Extent	Proportion of C2 elements that share given understanding
	Consistency of Shared Understanding	Proportion of key elements of shared understanding which are held in common
Flexible Synchronization	Adaptability	Time, effort and resources required to make a change
	Flexibility	Number and type of control mechanisms available
Simultaneous C2 Processes	Currency	Time required to propagate change of a mission to appropriate C2 elements
	Synchronization	Percentage of sub-elements simultaneously involved in the planning process
Dispersed Command	Congruence with Command Intent	Percentage of subordinates who can accurately articulate commander's intent
Responsive and Tailorable	Responsiveness	Time required to change organizational structure
	Appropriateness	Extent of match between organizational structure and task/mission
Integrated C2 Components	Accessibility of Information	Number of times critical information is denied
	Extent of Lexicon	Frequency of misunderstandings

Appendix IV - Examples of Symmetric and Asymmetric scenarios using the shared adversarial process model.

Battle of Midway – Symmetric Model

Positioned Mechanisms - Japan
160 NAVAL Vessels
8 Carriers
600 Planes

Positioned Mechanisms – US
76 NAVAL Vessels
700 Planes
3500 Crew
3 Carriers

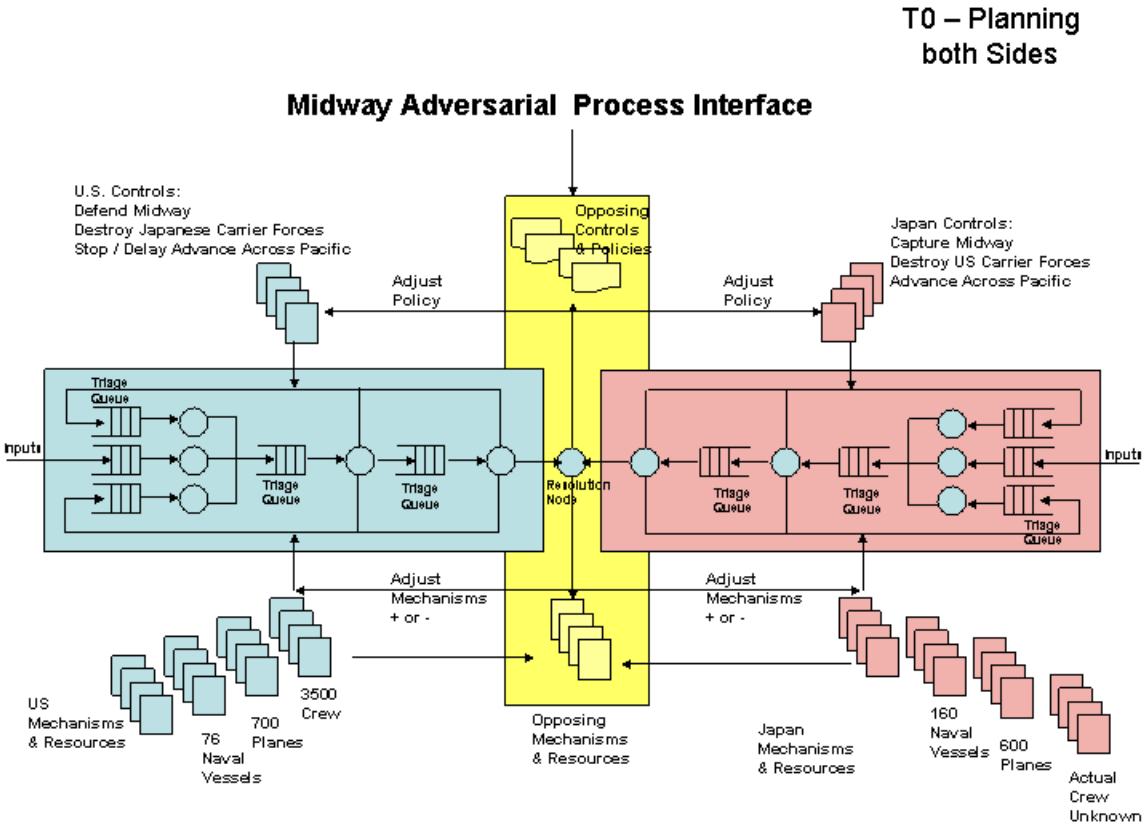


Figure 33 – Midway Model T0

Controls - Objectives - JAPAN
Capture Midway
Decoy US forces in Aleutians – Islands were in fact captured by Japan
Destroy US Carrier Resources
Objectives – US
Defend and Hold Midway
Destroy Japanese Carrier Resources
Block Japanese advance across Pacific

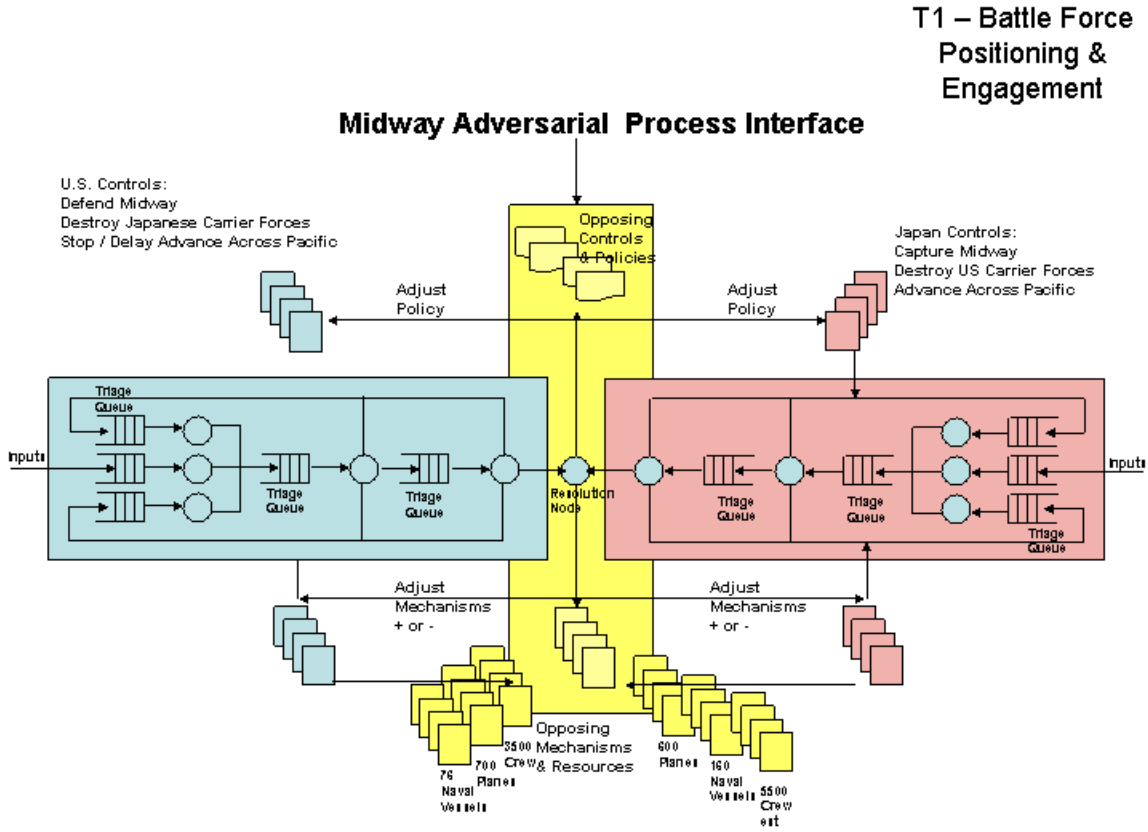


Figure 34 – Midway Model T1

Effects of Midway Operations
Japanese NAVAL Objectives Status

1. Midway not captured
2. 2 Aleutian Islands captured

Japanese Metrics

1. Mechanism re-alignment latency = weeks (distance from Japan)
2. Mechanism status –
    a. 253 planes lost
    b. 3500 lives lost
    c. 4 carriers lost

3. Superior decision status – Poor - lost objectives, lost large mechanism count, lost strategic advantage, withdrew Naval forces
4. Situational Awareness
    a. Japan had awareness of Friendly COA and Controls
    b. Japan had no or little awareness of Enemy COA and Controls
    c. Japan had knowledge of terrain
    d. Japan had little knowledge of U.S. force location (mechanism status)
    e. Japan had knowledge of friendly force location (mechanism status)
    f. Japan did not have total situational awareness
5. Single version of truth attributes – Unknown truth content – Poor situational awareness
    a. Incomplete - Enemy force (US) positions not well known
    b. Inaccurate – Force positioning decisions delayed

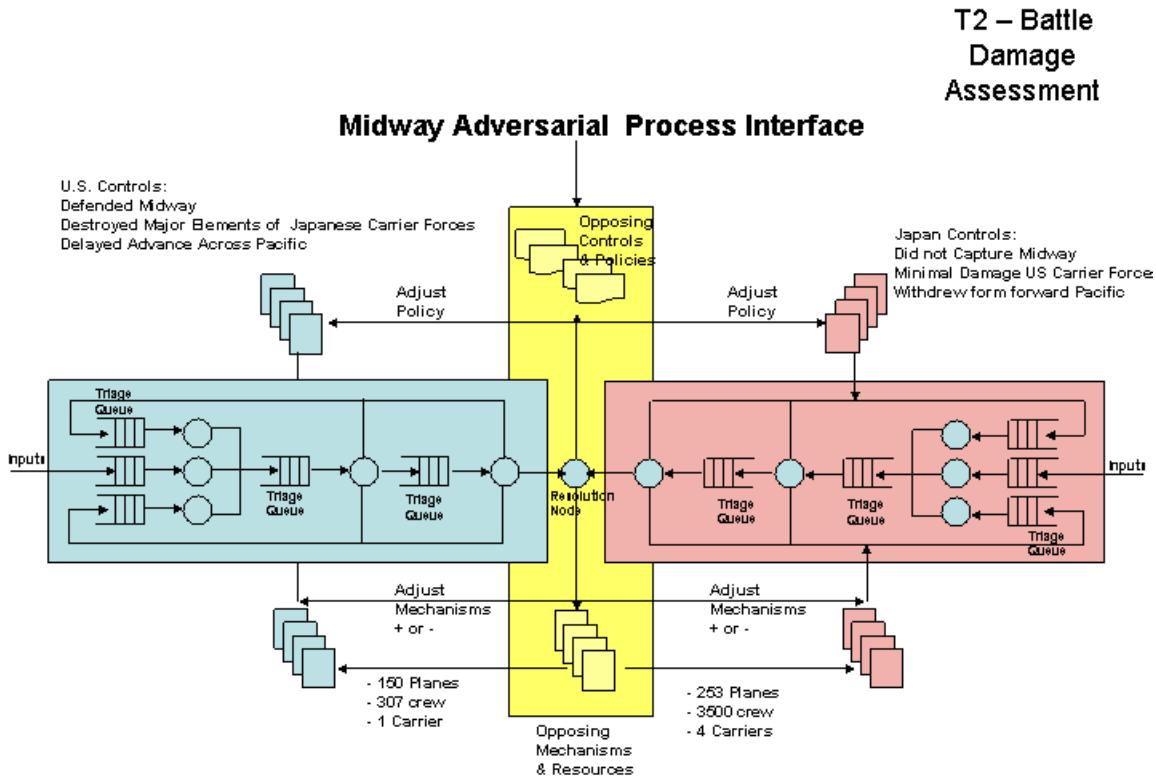


Figure 35 – Midway Model T2

US NAVAL Objectives Status

1. Midway Island held
2. Japanese advance across Pacific slowed

US Metrics

1. Mechanism re-alignment latency = days

2. Mechanism status –
   a. 150 Planes lost
   b. 307 lives lost
3. Superior decision status – Good gained objectives, lost fewer mechanisms than expected, gained strategic advantage, blocked Japanese Naval forces
4. Situational Awareness - good
   a. U.S. had awareness of Friendly COA and Controls
   b. U.S. had good awareness of Enemy COA and Controls
   c. U.S had knowledge of terrain
   d. U.S. had knowledge of Japanese force location (mechanism status)
   e. U.S. had knowledge of friendly force location (mechanism status)
   f. U.S. had total situational awareness
5. Single version of truth attributes – Known truth content
   a. Good - Enemy force (Japanese) positions well known

Battle of Thermopylae (the 300 Spartans) – Symmetric Model

Positioned Mechanisms – Persian Army
300,000 warriors

Positioned Mechanisms – Greece & Sparta
1500 Greek Warriors
300 Spartan Warriors

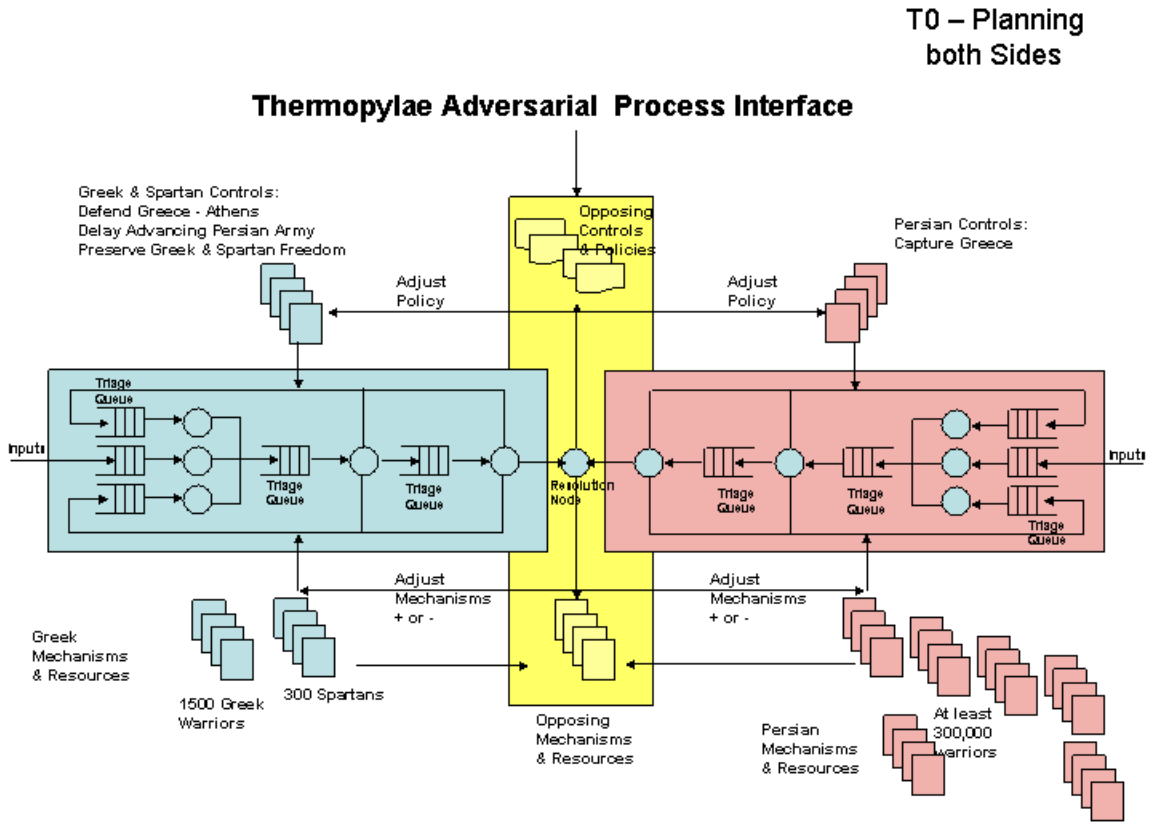


Figure 36 – Thermopylae Model T0

Objectives - Persia
Capture Greece & Sparta
Avenge loss by Father
Expand Persian Control

Objectives - Greece
Defend Greece & Sparta
Preserve Athenian Democracy & Freedom

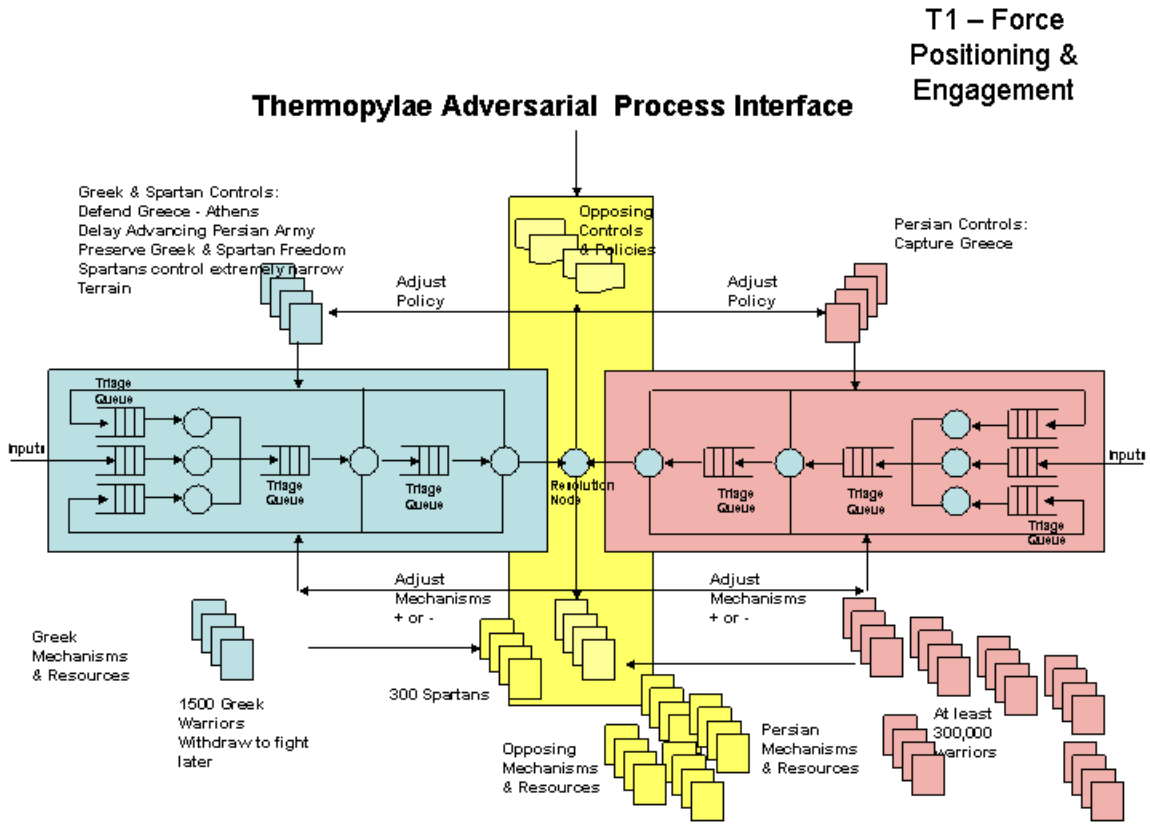


Figure 37 – Thermopylae Model T1

Effects of Persian Operations

Persian Objectives Status

1. Conquest of Greece delayed due to heavy losses inflicted by Spartans
2. Delay in attacking Athens
3. Absorbed 20,000 - casualties

Greek Objectives Status

1. Delay of Persian Army successful in allowing Greek Army time to prepare

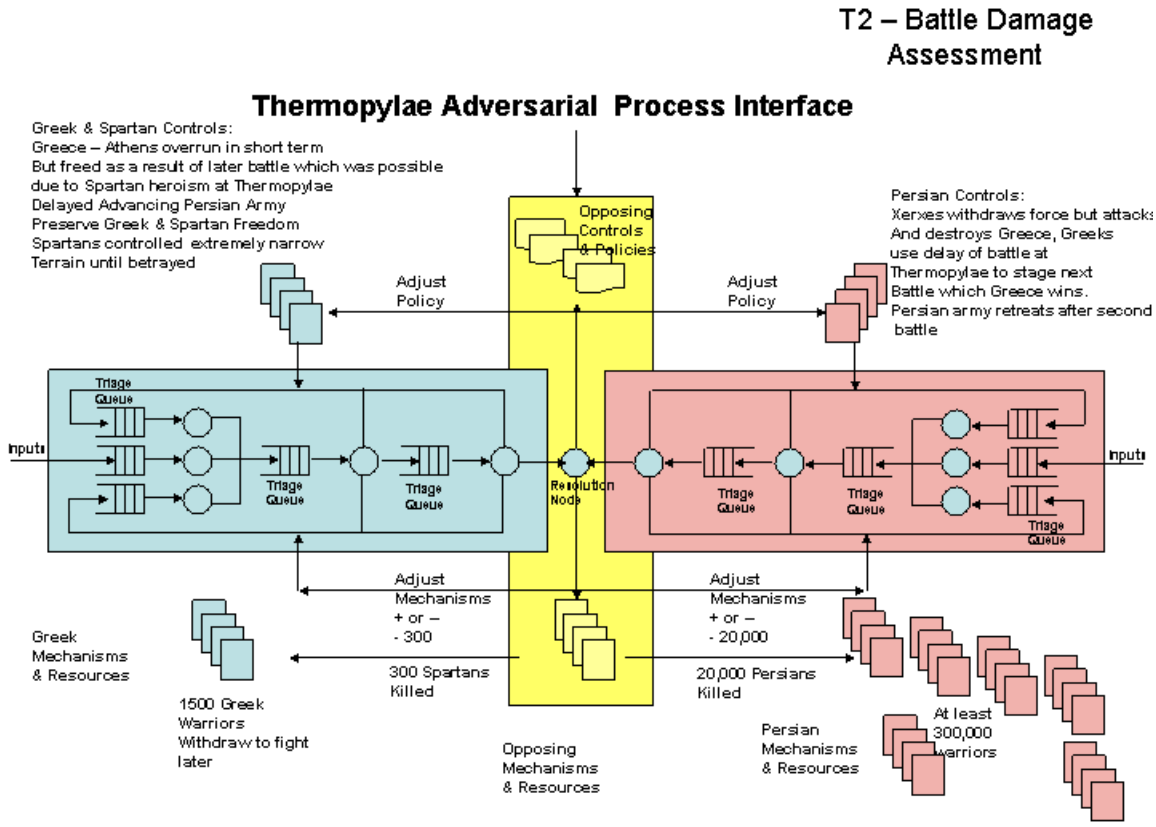


Figure 38 – Thermopylae Model T2

Greek Metrics

1. Mechanism re-alignment latency = days
2. Mechanism status –
   a. 1500 Greek warriors withdrawn to fight later
   b. 300 Spartan lives lost
3. Superior decision status – Strategically Good - gained objectives, lost fewer mechanisms than expected, gained strategic advantage, delayed Persian advance to permit Greek forces to regroup, tactically questionable since all Spartan forces perished
4. Situational Awareness – good
   a. Greece had awareness of Friendly COA and Controls
   b. Greece had good awareness of Enemy COA and Controls
   c. Greece had knowledge of terrain
   d. Greece had knowledge of Persian force location (mechanism status)
   e. Greece had knowledge of friendly force location (mechanism status)
   f. Greece had total situational awareness
5. Single version of truth attributes – Known truth content
   a. Good - Enemy force (Persians) positions well known
   b. Good – Persian Troop Strength known

Persian Metrics

1. Mechanism re-alignment latency = weeks
2. Mechanism status –
   a. 20,000 Persian lives lost
3. Superior decision status – Strategically & tactically poor- gained short term objectives but at a high mechanism count, delay permitted Greek forces to regroup, tactically questionable loss of 20,000 men
4. Situational Awareness – good but not as good as the Greeks
   a. Persians had awareness of Friendly COA and Controls
   b. Persians had minimum awareness of Enemy COA and Controls
   c. Persians had poor knowledge of terrain
   d. Persians had knowledge of Greek force location (mechanism status)
   e. Persians had knowledge of friendly force location (mechanism status)
   f. Persians had less situational awareness than the Greeks
5. Single version of truth attributes – Known truth content
   a. Fair - Enemy force (Greeks) positions well known
   b. Fair – Greek – Spartan Troop Strength known but underestimated in ability

Battle of Okinawa Asymmetric – Symmetric Model

Positioned Mechanisms – Japan
120,000 men
8000 planes
20 Naval Vessels
(Included Yamato, Cruisers, and 8 Destroyers)

Positioned Mechanisms – U.S.
538,000 men
1457 Naval Vessels
700 Planes

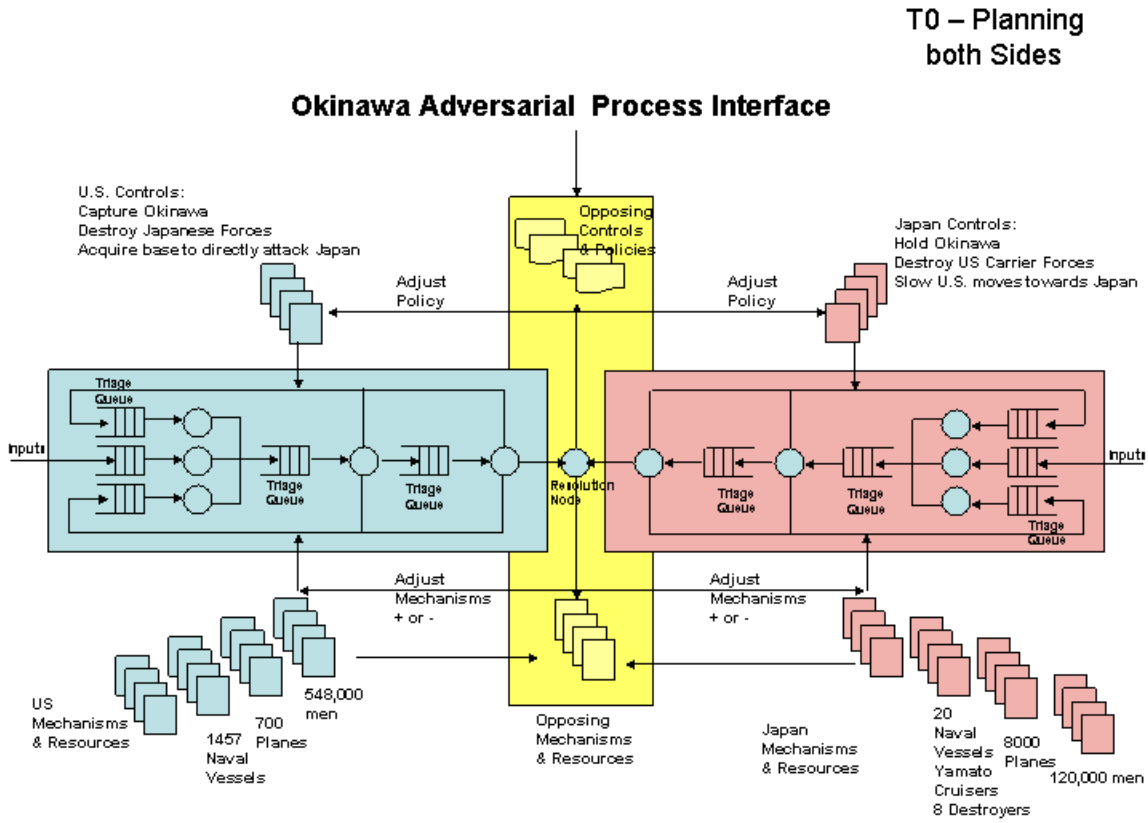


Figure 39 – Okinawa Model T0

Objectives – Japan
Hold Okinawa
Destroy U.S. Carrier Forces
Slow U.S. moves towards Japan
Inflict heavy losses

Objectives – U.S.
Capture Okinawa as invasion of Japan base
Destroy Japanese Forces

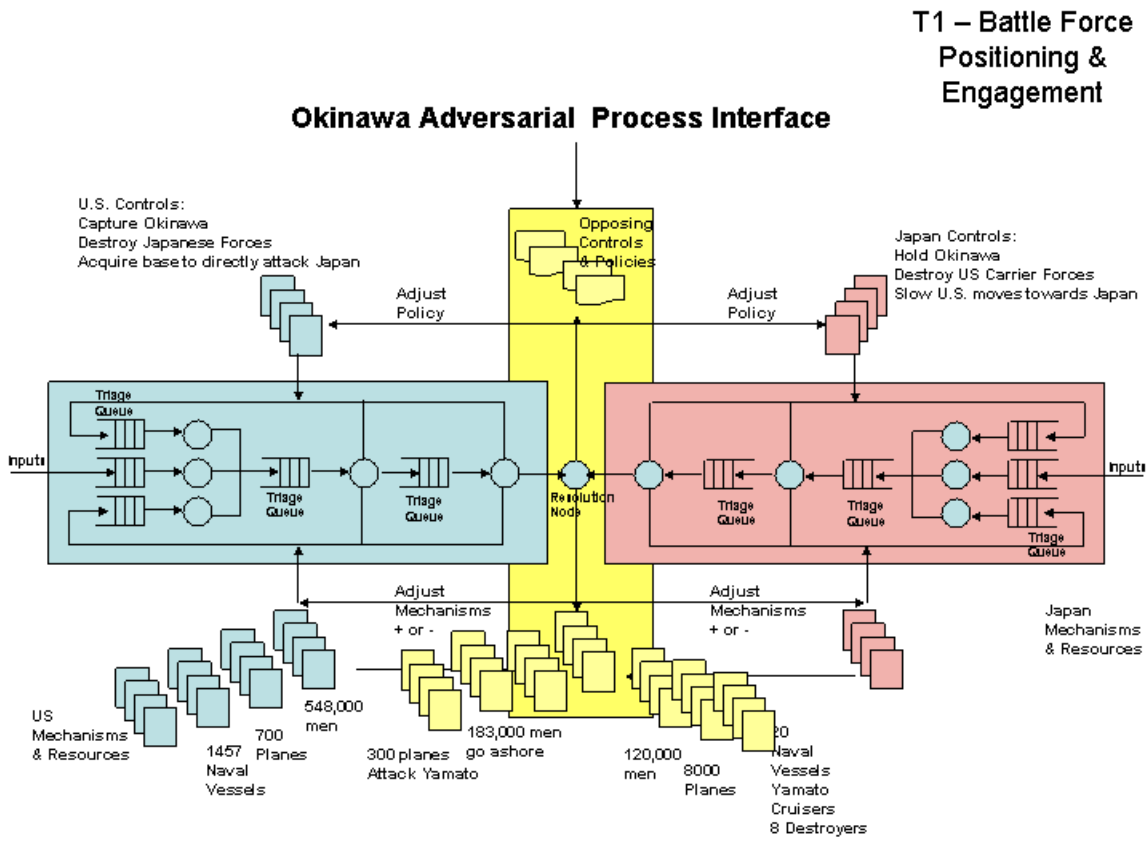


Figure 39 A – Okinawa Model T1

Effects of Okinawa Operations

Japanese NAVAL Objectives Status

1. Okinawa Lost
2. Inflicted heavy casualties on U.S.
3. This helped make case for dropping atomic bomb

Japanese Metrics

1. **Mechanism re-alignment latency = days (distance from Japan)**
2. **Mechanism status –**
    a. 7800 planes lost – 1465 lost as kamikaze
    b. 120,000 Japanese KIA
    c. 42,000 Okinawa civilians killed
    d. Yamato sunk – all hands 3000 lost
    e. All cruisers and 8 destroyers sunk
3. **Superior decision status –** Poor - lost objectives, lost large mechanism count, lost strategic advantage, lost major Naval forces
4. **Situational Awareness**
    f. Japan had awareness of Friendly COA and Controls
    g. Japan had no or little awareness of Enemy COA and Controls
    h. Japan had knowledge of terrain
    i. Japan had knowledge of U.S. force location (mechanism status)

j. Japan had knowledge of friendly force location (mechanism status)
k. Japan did have total situational awareness

5. **Single version of truth attributes – Known truth content**
   a. Complete - Enemy force (US) positions well known

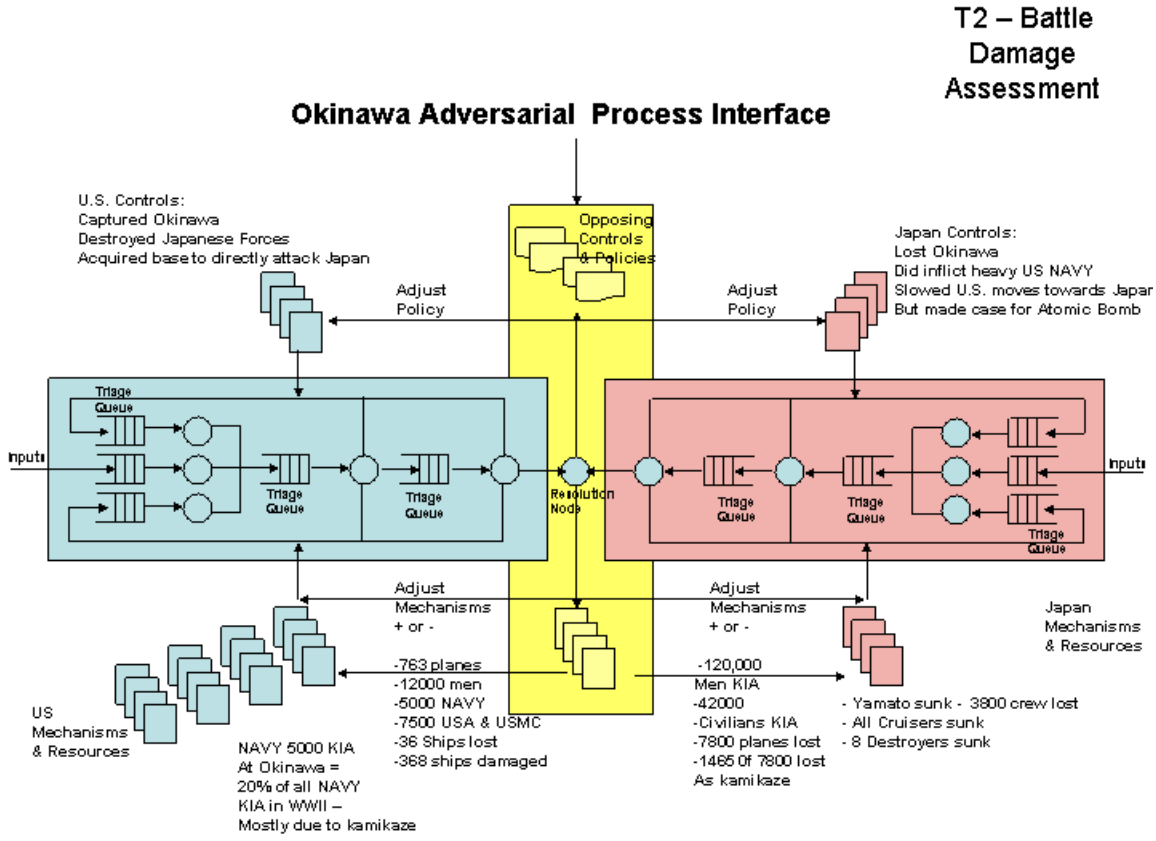


Figure 40 – Okinawa Model T2

Effects of Okinawa Operations

U.S NAVAL Objectives Status

1. Okinawa captured
2. Inflicted heavy casualties on Japanese military
3. This helped make case for dropping atomic bomb

U.S. Metrics

1. Mechanism re-alignment latency = days (distance from Japan)

2. Mechanism status –
   a. 763 planes lost
   b. 12,000 U.S KIA
   c. NAVY KIA - 5,000 (20% of all Navy KIA in WWII due to Kamikaze)
   d. USA & USMC – 7500 KIA
   e. 36 ships lost
   f. 368 ships damaged

3. Superior decision status – Good - gained objectives, strategically wise, tactically expensive, lost large mechanism count, gained strategic advantage, lost significant Naval KIA
4. Situational Awareness
    a. U.S had awareness of Friendly COA and Controls
    b. U.S. had poor awareness of Enemy COA and Controls (willingness to use suicidal Kamikaze squads)
    c. U.S had knowledge of terrain
    d. U.S. had some knowledge of Japanese force location (mechanism status)
    e. U.S. had knowledge of friendly force location (mechanism status)
    f. U.S. had fair total situational awareness
5. Single version of truth attributes – Unknown truth content – Poor COA understanding of Japanese intentions to use Kamikaze squads
    a. Complete - Enemy force positions well known

Attacks of September 11, 2001– Asymmetric Model

Positioned Mechanisms – Al-qaeda
Cell membership totals unknown

Positioned Mechanisms – U.S. (Accidentally positioned)
U.S. civilian financial markets
U.S. DoD Headquarters at the Pentagon
U.S. civilian & commercial air fleets

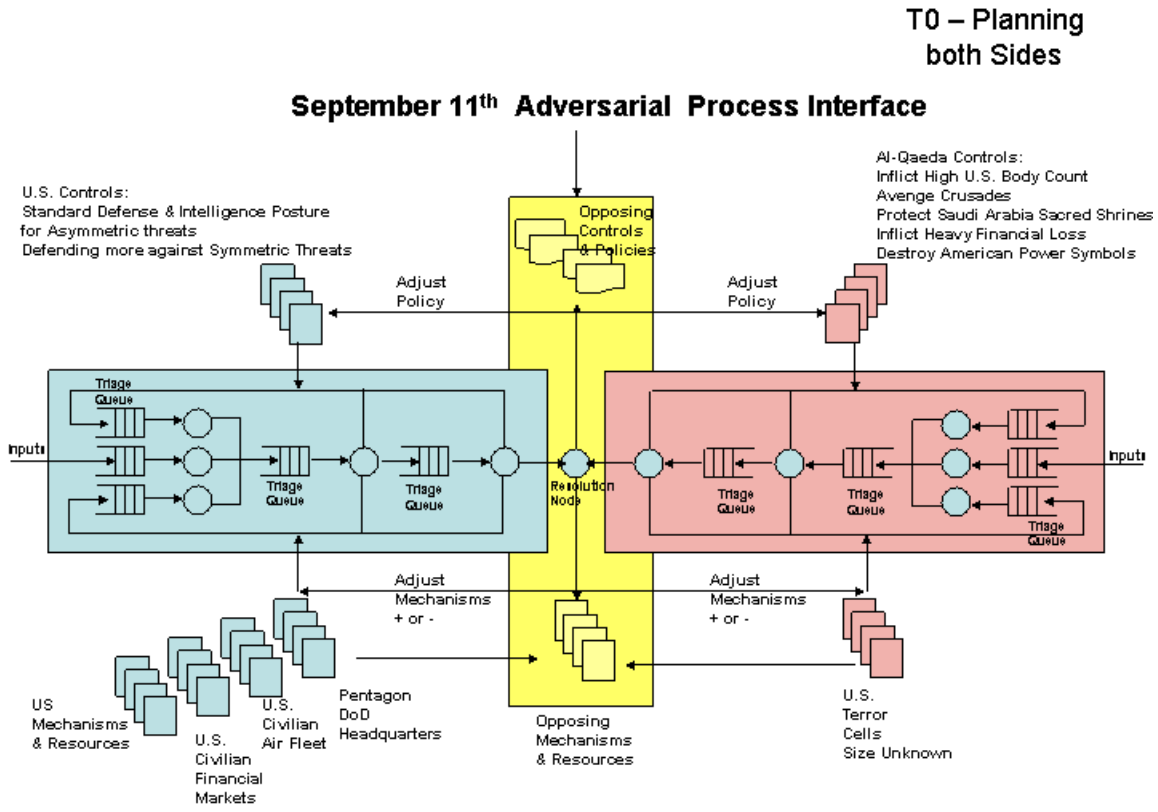


Figure 41 – September 11th Model T0

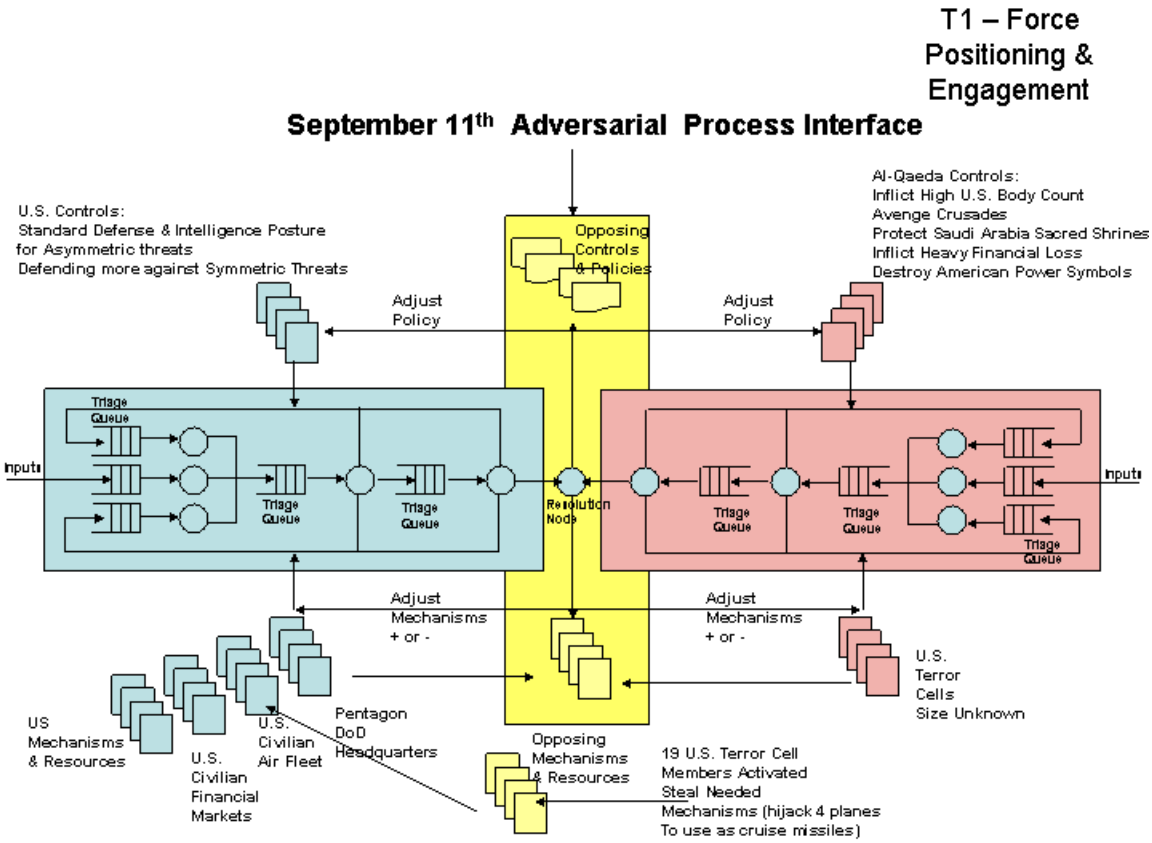


Figure 42 – September 11th Model T1

U.S. Controls
Standard Defense & Intelligence Posture for Asymmetric threats
Defending more on symmetric threats

Al-Qaeda Controls
Inflict High U.S. body count
Avenge Crusades
Protect Saudi Arabia Sacred Grounds
Inflict Heavy Financial Loss
Destroy American Power Symbols

Effects of September 11th 2001 Operations
Al-Qaeda Objectives Status

1. Pentagon struck with airplane used as cruise missile
2. Inflicted heavy casualties in New York City Trade Center Attack
3. Caused massive destruction in New York City Trade Center Attack
4. Inflicted major financial damage
5. Destroyed U.S. capitalism power symbol in NYC

Al-Qaeda Metrics

1. Mechanism re-alignment latency = hours (cell activation estimate)
2. Mechanism status –
    a. 19 cell members died
    b. $1,000,000.00 funding required
3. Superior decision status – Good - achieved objectives, lost minimum mechanism count, gained surprise temporary strategic advantage
4. Situational Awareness
    a. Al-Qaeda had awareness of Friendly COA and Controls
    b. Al-Qaeda had good awareness of Enemy COA and Controls
    c. Al-Qaeda had knowledge of terrain
    d. Al-Qaeda had knowledge of U.S. force location (mechanism status)
    e. Al-Qaeda had knowledge of friendly force location (mechanism status)
    f. Al-Qaeda did have total situational awareness
5. Single version of truth attributes – Known truth content
    a. Complete - Enemy force (US) positions well known

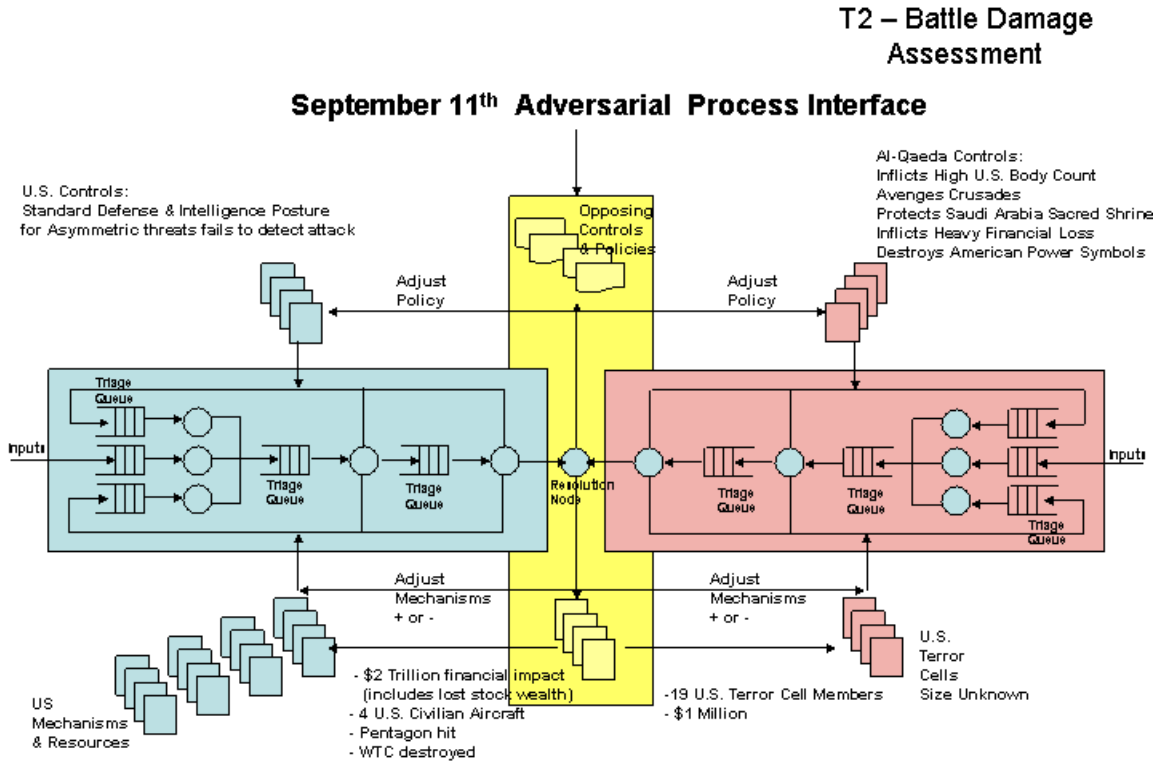


Figure 43 – September 11th Model T2

U.S. Metrics

1. Mechanism re-alignment latency = hours
2. Mechanism status –
    a. 3000 civilians killed
    b. $2,000,000,000,000.00 in damages with $1.7 trillion lost in financial markets
    c. 4 U.S. aircraft stolen as used as cruise missiles
    d. Pentagon bombed with stolen aircraft used as cruise missile
    e. World Trade Centers bombed and destroyed with stolen aircraft used as cruise missile
3. Superior decision status – Extremely poor – U.S. not defended, high lost mechanism count, Al-Qaeda surprised intelligence assets
4. Situational Awareness
    a. U.S had awareness of Friendly COA and Controls
    b. U.S had poor awareness of Enemy COA and Controls
    c. U.S. had knowledge of terrain
    d. U.S. had no knowledge of enemy force location (mechanism status)
    e. U.S. had knowledge of friendly force location (mechanism status)
    f. U.S. had no total situational awareness
5. Single version of truth attributes – Unknown truth content
    a. Incomplete - Enemy force COA & positions not known

Appendix V – Service Level Agreements and A Quality of Service XML Schema

Service-Level Agreement (SLA)

A service-level agreement (SLA) is a formal contract between a service provider and a client guaranteeing quantifiable process performance at defined levels. SLAs can be either very general or extremely detailed, and generally include the steps that should be taken by the service provider and the client in the event of failure. The service provider guarantees that the service it provides will be available for a certain maximum and average response times. The client obtains rights and specified time periods. The client also agrees to accept specified exceptions to the general terms of the agreement. These rights, remedies, and exceptions vary from one SLA to another.

Exceptions

An SLA will usually specify exceptions to its terms. Exceptions can be divided into four areas: failures, network issues not within the direct control of service provider, denial of service, and scheduled maintenance. Examples of these categories can be found in Table 1. Other exceptions can be added to suit a provider's situation, as long as the clients can get reasonable compensation for downtime. By providing exceptions in an SLA, a provider can protect itself from liability in case of problems or network outages.

Table 1 - Exception Examples

Type	Examples
Failures	Hardware failure Telecommunication failure Software bugs/flaws Monitoring/measurement system failure
Network issues not within direct control of service provider	Backbone peering point issues DNS issues not within control of service provider
Denial of service	Client negligence/willful misconduct Network floods, hacks, and attacks Acts of God, war strikes, unavailability of telecommunications, inability to get supplies or equipment needed for the provision of the SLA
Scheduled maintenance	Hardware upgrades Software upgrades Backups

Quality of Service

Delivering Quality of Service (QoS) on the Internet is a critical and significant challenge because of its dynamic and unpredictable nature. Applications with very different characteristics and requirements compete for scarce network resources. Changes in traffic patterns, denial-of-service attacks and the effects of infrastructure failures, low performance of Web protocols, and security issues over the Web create a need for Internet QoS standards. Often, unresolved QoS issues cause critical transactional applications to suffer from unacceptable levels of performance degradation. By QoS, we refer to non-functional properties of Web services such as performance, reliability, availability, and security.

- **Availability:** Availability is the quality aspect of whether the Web service is present or ready for immediate use. Availability represents the probability that a service is available. Also associated

with availability is time-to-repair (TTR). *TTR* represents the time it takes to repair a service that has failed. Ideally smaller values of TTR are desirable.

- **Accessibility:** Accessibility is the quality aspect of a service that represents the degree it is capable of serving a Web service request. It may be expressed as a probability measure denoting the success rate or chance of a successful service instantiation at a point in time.
- **Integrity:** Integrity is the quality aspect of how the Web service maintains the correctness of the interaction in respect to the source.
- **Performance:** Performance is the quality aspect of Web services, which is measured in terms of throughput and latency. *Throughput* represents the number of Web service requests served at a given time period. *Latency* is the raound0trip time between sending a request and receiving the response.
- **Reliability:** Reliability is the quality aspect of a Web service that represents the degree of being capable of maintaining the service and service quality. The number of failures per month or year represents a measure of reliability of a Web service.
- **Regulatory:** Regulatory is the quality aspect of the Web service in conformance with the rules, the law, compliance with standards, and the established service level agreement.
- **Security:** Security is the quality aspect of the Web service providing confidentiality and non-repudiation by authenticating the parties involved, encrypting messages, and providing access control.

Dynamic QoS

In a dynamic QoS model, the QoS requirements are embedded in the XML Message Meta Data. The QoS Meta data tags can define such things as an end-to-end transmission time not to exceed x milliseconds. The XML message could be "time stamped" at transmission and then compared to the arrival time stamp at the destination. Using a dynamic QoS can demonstrate whether or not certain requirements currently being met (such as Real Time data transfer) by legacy systems are actually enhanced or degraded by Fn.

QoS Meta Tags

Meta tags for Quality of Service should be added to the header of each message. The tags will specify the non-functional properties of the message.

QoS DTD

```
<!DOCTYPE QoS[
<!ELEMENT QoS (Availability, Accessibility, Integrity,
               Performance, Reliability, Regulatory,
               Security)
>
<!ATTLIST QoS SLA CDATA #IMPLIED>
<!ELEMENT Availability (#PCDATA)>
<!ATTLIST Availability TTR CDATA #IMPLIED>
<!ELEMENT Accessibility (#PCDATA)>
<!ATTLIST Accessibility Scalability (High | Medium | Low) #IMPLIED>
<!ELEMENT Integrity (#PCDATA)>
<!ELEMENT Performance (Throughput, Latency)>
<!ELEMENT Throughput (#PCDATA)>
<!ELEMENT Latency (#PCDATA)>
<!ELEMENT Reliability (#PCDATA)>
<!ELEMENT Regulatory (Standard*)>
<!ELEMENT Standard EMPTY>
<!ATTLIST Standard Name CDATA #REQUIRED
                   Version CDATA #IMPLIED
>
<!ELEMENT Security (#PCDATA)>
]>
```

Example XML from QoS DTD

```
<QoS SLA=”ProviderX-SLA-ver2_1.doc”>
    <Availability TTR=”3”>75</Availability>
    <Accessibility Scalability=”High”>87</Accessibility>
    <Integrity>Medium</Integrity>
    <Performance>
        <Throughput>4500</Throughput>
        <Latency>.01</Latency>
    </Performance>
    <Reliability>84.3</Reliability>
    <Regulatory>
        <Standard Name=”SOAP” Version=”1.1”>
    <Regulatory>
    <Security>Level4 Authentication</Security>
</Qos>
```

Resources

- Myerson, Judith M., “Guarantee your Web service with an SLA”, IBM developerWorks.
- Mani, Anbazhagan and Arun Nagarajan, “Understanding quality of service for Web sservices”, IBM developerWoks.

Appendix VI – A few observations concerning Service Oriented Architectures and the migration away from legacy systems

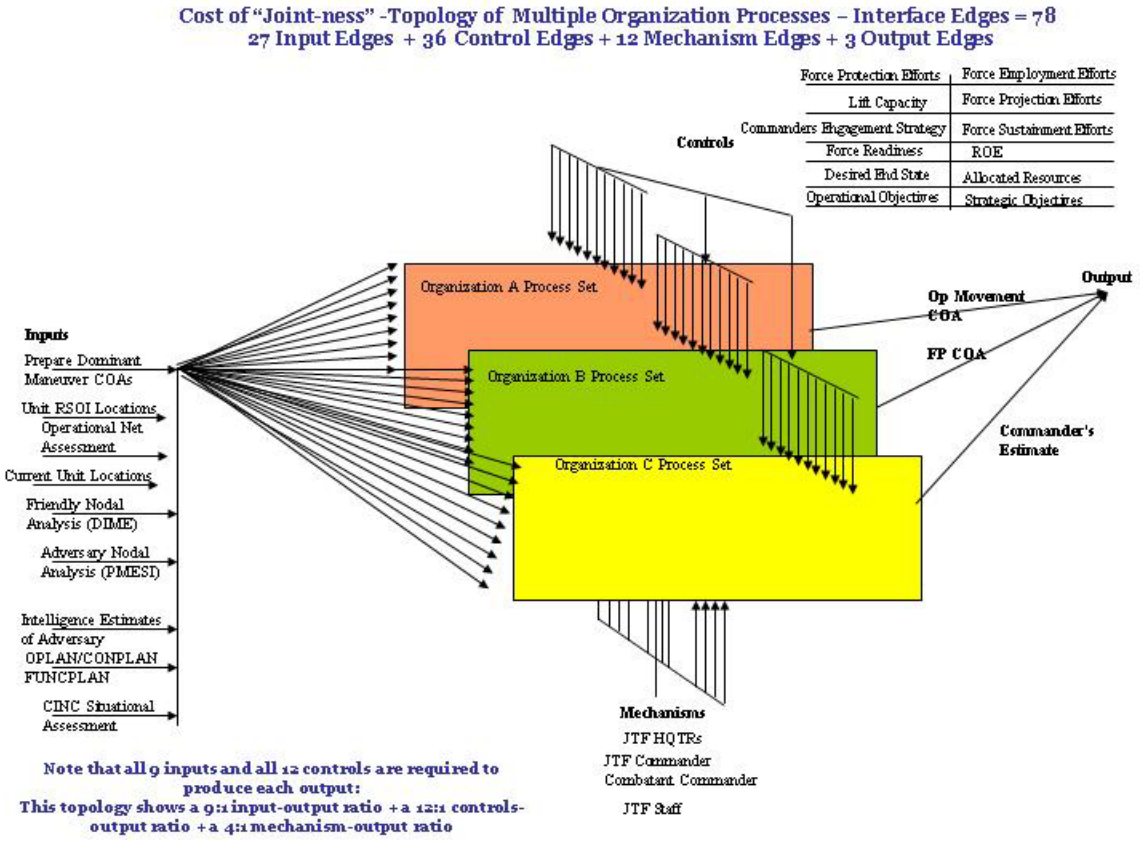


Figure 44 – Dominant Maneuver – Force Positioning Topology

In the above graphic, it should be noted that each of the 12 controls and 9 inputs required to create "just" the force positioning output are each individualized published services. The process nodes internal to each organization shown must contain "subscriber services" capable of processing the published data. Then, there must be at least 3 nodes containing services which publish the final formatted outputs. A "bare minimum" of 27 content processing, publishing and subscribing services must exist on top of a Service Oriented Architecture (SOA) capable of providing tens of enabling infrastructure services required to allow the necessary content service orchestration. Some one must have created the 27 control and input services and maintains the enabling infrastructure services before a single commander's estimate can be produced. These are just a few thoughts for SOA designers planning to rip out the functions contained in current legacy systems and expose those capabilities on the Global Information Grid (GIG) and then "retire" the legacy systems. Since the above services will probably be subscriptions managed by a specific Community of Interest (per Dr. Paul's comments in the above appendix), it is easy to estimate that over 100 services will be required to

support the "flattening" of legacy stovepipes into a SOA just for this COA which is concerned about force planning.

Appendix VII - Jim Saxton (R-NJ), Chairman Joint Economic Committee, United States Congress, May 2002: "The Economic Costs of Terrorism"

COST AND ECONOMIC EFFECTS OF THE SEPTEMBER TERRORIST ATTACKS

The terrorist attack of September 11 imposed a number of significant costs on the economy and thereby substantially changed the economic outlook. These costs can be classified into three categories of both short- and long-term costs.

Short-term Costs:

• **Immediate Loss of Human and Nonhuman Capital:** As noted, the human costs have been horrendous. In addition to these human costs, the immediate and most obvious short-term economic costs result from the loss of life and loss of productive capacity of those killed. Additionally, the destruction of capital; the destruction of buildings, surrounding buildings, infrastructure, airplanes, and other public and private property of building tenants and others was substantial. Cleanup and repair costs also were substantial. Important and severe as these costs were, however, they constitute a relatively small percentage of the total physical and human capital assets of the U.S. economy as a whole.1

• **Effects of Uncertainty on Consumer and Investor Behavior:** Another category of short-term costs relates to the effects of increased uncertainty and its impact on consumer and investment behavior. An immediate effect of the terrorist attack, after all, was a dramatic increase in uncertainty and apprehension which became evident in financial markets. In effect, a sharp upward repricing of risk occurred. Increased uncertainty usually increases market volatility, thereby boosting risk premiums. This normally affects behavior; it induces investors, for example, to move out of riskier assets (such as stocks and speculative grade bonds) into safer, more liquid, and shorter-term assets (such as short-term U.S. Treasury securities, gold, or cash). It tends to adversely impact the stock market as well as commitments for long-term investments and purchases and to boost demand for short-term liquidity, which works to lower spending.

This increased uncertainty has negative impacts on consumption and investment as consumer and business confidence deteriorates. Discretionary consumer purchases such as long-lived consumer durables (e.g., cars, major appliances, etc.) or vacations and travel as well as long-term business commitments are often postponed or canceled as purchasers retrench and demand contracts. Additionally, related stock market declines reduce consumption (via negative wealth effects) and investment (via a higher cost of capital).

• **Effects of Retrenchment on Specific Industries or Localities:** These retrenchments in consumer and investment spending can have concentrated (adverse) impacts on certain industries. Thus, another category of short-term

costs pertain to the abnormal losses suffered by certain directly impacted industries, sectors, localities or regions. The September 11 attacks did have immediate and concentrated impacts on a number of industries: most notably, airlines, aerospace, travel, tourism, insurance, lodging, restaurants, recreation, gambling casinos and related

activities. These industries suffered concentrated economic and job losses. Of course, regions or localities with heavy concentrations of these industries suffered disproportionately as well.

Long-term Costs:

There are significant long-term economic costs of terrorism as well. The economic costs of a permanently increased, ongoing terrorist threat will be important and may very well bring major changes to our way of life. These long-term effects may be classified into three categories of costs.

• **Increased costs of security analogous to a "security" or "terrorist tax":** Part of these additional long-term security costs entail added delays, inefficiencies, and frictions and have effects similar to an added transaction tax on the economy. In effect, these costs will be analogous to a "security" or "terrorist tax" on the economy, and impose an adverse supply-side impact on the economy.

Such costs will take many forms and entail multiple dimensions. A cursory list would include travel delays, additional security checks and inspections, longer cross-border transfers, higher insurance costs, additional informational requirements, higher construction costs, intelligence agency upgrades, higher shipping costs, more regulation, the maintenance of higher levels of inventories (as insurance against supply disruptions), immigration restrictions, slower mail deliveries, and a myriad of other costs. These various costs, while essential, do nothing to increase the quantity or quality of the supply of goods or services. In fact, these measures will raise the cost of doing business, stifle gains from free exchange, add inefficiencies, and hence constitute a negative supply-side shock or added "tax" on the economy. As a consequence, the real return to capital will decline and over time, these costs may adversely impact both the economy's productivity growth and long-term potential growth rate.

• **Anti-Terrorist Expenditures Crowd Out More Productive Activity:** Another form of longer-term costs of security involves the opportunity cost of spending additional money to fight terrorism. After the September 11 attacks, a variety of new spending on security occurred. As this happens, economic resources will be directed to shoring up security and diverted away from more productive private sector activity. These expenditures involve necessary security spending to shore-up buildings, intelligence, and defense. More specifically, it involves expenditure for security guards, guards dogs, building fortifications and barriers, metal bomb detectors, and a myriad of other security devices. It will involve the costs of backup site and facility maintenance, contingency and disaster planning, better training, increased screening and hiring, and increased mail security.

The costs of protection against bio-chemical terrorism also will be significant and will call for expenditures of a different type. For example, the costs of developing inoculations, providing antibiotics, and developing treatments will be significant. Our "anthrax scare" experience has shown that the costs of protecting private and public sector mail delivery services including mail handlers, of installing detection devices, and of providing medical care and insurance can be significant. The costs of screening for exposure to and infection by bioterrorist agents such as anthrax can also be substantial. As a consequence of this increased security spending and associated crowding out of more productive activity, the total private productive capital stock will be less than it would otherwise have been. The so-called "peace dividend" – a dividend that freed up

resources for additional private sector growth – is lessened. In short, monies for a necessary security buildup crowd out more productive private investment. Consequently, the long-run costs of combating terrorism to some extent involve adverse effects to the private capital stock and thereby aggregate supply, productivity, and the long-run potential growth rate of the economy.

• **Other long-run costs:** Another catch-all category of long-run costs of terrorism is "other long-run costs." This includes the hard to measure long-run costs of added anxiety, stress, and mental disorders associated with the increased uncertainties of, and permanent threat of, terrorism as well as the costs of alternative forms of terrorism (e.g., bio-, nuclear-, or cyber-terrorism.)

SOME ROUGH, PRELIMINARY ESTIMATES OF THE COSTS OF SEPTEMBER 11

A number of studies have come up with preliminary estimates of the costs of the September 11 terrorist attacks in the U.S. In general, the cost estimates of these studies cannot be directly compared and contrasted with one another for a number of reasons. For the most part, for example, these studies are imprecise, providing "back of the envelope" or rough orders of magnitude estimates. The studies make differing assumptions, measure different categories and alternative dimensions of costs, define and aggregate these costs differently, and are not comprehensive. Nonetheless, a summarization of these efforts is instructive in identifying both rough orders of magnitude of these costs and their uncertainty as suggested by the wide range of estimates. The following summary categorizes these costs as outlined above.

Short-term cost estimates

Immediate Loss Estimates: Becker and Murphy estimate the immediate loss of human and non-human capital to be in the range of $25 billion to $60 billion, or about 0.2 percent of the economy's physical assets and 0.06 percent of total productive assets.[3] A study by the Milken Institute put property damage at $10 billion to $13 billion and human capital losses on the order of $40 billion. An International Monetary Fund (IMF) study identifies the direct costs of the September 11 attacks as totaling about $21.4 billion (including direct insurance costs) or about 0.25 percent of GDP.

Estimates of Short-Term Lost Economic Output: Early, preliminary estimates of lost economic output resulting from the terrorist shock were provided by a Milken Institute study. ***This study estimated lost economic output in the immediate aftermath of the attack at $47 billion and lost stock market wealth at $1.7 trillion***. From the benefit of hindsight, however, these short-term effects of uncertainty on economic behavior have apparently proven to be temporary partly because of an adept and rapid offsetting policy response, early success of the war on terrorism, and because, thankfully, we have not experienced another terrorist

Appendix VIII - DONCIO Glossary

- **Surveillance** Definition: The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. Source: JPUB 1-02Reference:Department of Defense, Joint Publication 1-02: DOD Dictionary of Military and Associated Terms, 23 March 1994 as amended 15 April 1998.Subject Area: DoD terms
- **Reconnaissance** Definition:(JCS) A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. See also aerial reconnaissance; hydrographic reconnaissance; radar reconnaissance; triangulation reconnaissance.
- **Intelligence** Definition: 1. Product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
- **Command and Control** Definition: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

References:

1. **Source: http://www.wpafb.af.mil/museum/history/wwii/pha.htm**
2. **Sources: CNN & Reuters & September11News.com.**
3. **Jim Saxton (R-NJ), Chairman Joint Economic Committee, United States Congress, May 2002: "The Economic Costs of Terrorism**
4. **Source: The Institute for Analysis of Global Security.**
5. **Smith, Edward A., Effects Based Operations – pp 76,78**
6. **David S. Alberts, John J. Garstka, and Frederick P. Stein: Network Centric Warfare. CCRP Publications**
7. **National Institute of Standards: FIPS 183, 1993, IDEF model definition**
8. **H.Van Dyke Parunak: *The Process-Interface-Topology Model: Overlooked Issues in Modeling Social System*, 2000, ERIM Center for Electronic Commerce**
9. **Ravindra Krovi et al, Information Flow Parameters for Managing Organizational Processes.**
10. **Micheal Fyall: When Project Information flow Becomes Turbulent: Towards an Organizational Reynolds Number. CIFE Technical Report #138, August 2002, Stanford University**
11. **Mayfield, Terry and Larsen, Greg, IDA Corporation, personal correspondence, December 12, 2003**
12. **Hackerthorn, Richard: Factors for Implementing Active Data Warehousing, 7/28/2003, available at datawarehouse.com**
13. **St. Augustine: On The Trinity, page 377, book 14, New City Press, 1997.**
14. **Mayfield, Terry : Dominant Maneuver Architecture Working Group Interim Progress Review , 25 April 2002**
15. **Dawkins, Richard :"The Extended Phenotype", New York, Oxford University Press, 1989**
16. **Qiao, Liang - Wang, Xiangsui, Senior Colonels People's Liberation Army: Unrestricted Warfare, Beijing, 1999 – Pan American Publishing Company, Panama City, Panama**
17. **Bertsekas, Dimitri - Gallagher,Robert - Massachusetts Institute of Technology: Data Networks, Prentice Hall, 1987**
18. **Alberts, David – Hayes Richard: "Power to The Edge, Command and Control in the Information Age"**
19. **Holland, John: "Adaptation in Natural and Artificial Systems", a Bradford Book, MIT Press, 1992**
20. **Downing, Keith Norwegian University of Science and Technology and Zvirinsky, Peter Technical University of Kosice, Slovakia: The Simulated Evolution of Biochemical Guilds: Reconciling Gaia Theory and Natural Selection**
21. **Paul, Raymond PhD, Office of the Assistant Secretary of Defense for Networks Information and Integration: personal correspondence, February 2004**

22. Sheehan, Jack et al: The Military Missions and Means Framework, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2003
23. Pacetti, Don, Cmdr USN Retired: Personal Correspondence, March 2004